Question Bank

UNIT - I

[3 Marks]

1. Define cloud computing and list any two of its essential characteristics.
2. What is meant by Region in AWS Global Infrastructure? List the Regions available in India.
3. Differentiate between public cloud and private cloud (any two differences).
4. In the AWS Shared Responsibility Model, give two examples of customer responsibilities.
5. What is an Availability Zone (AZ) in AWS? List the number of AZ's available in India.
6. Define AWS Identity and Access Management (IAM) and its purpose.
7. Explain the function of IAM in managing access to AWS resources.
8. Define IAM policy and its role in access control.
9. Define an IAM user and explain its use in AWS.
10. Explain the purpose of IAM groups in user management.
11. Define how policies are used to assign permissions to IAM users or groups.
12. Define an IAM role and explain its primary use.
13. Explain the difference between an IAM role and an IAM user.
14. Define a situation where assigning an IAM role is preferable over creating a new IAM user.
15. Explain the importance of enabling Multi-Factor Authentication (MFA) for IAM users.
16. Explain why it is best practice to avoid using the root account for daily tasks

[5 marks]

1. List and explain any five advantages of cloud computing over traditional on-premises computing.
2. Describe the three main cloud service models: IaaS, PaaS, and SaaS with examples.
3. Explain the components of AWS Global Infrastructure (Region, AZ, Edge Location, Local Zone) by AWS.
4. Compare traditional on-premises computing with cloud computing in terms of cost, scalability, and maintenance.
5. Explain the core features of AWS Identity and Access Management and how they support secure access control.

6. Describe the structure and working of IAM, including its integration with AWS services.
7. Explain how IAM users and groups are managed and how policies are attached to them.
8. Describe the process of assigning permissions to a group and how those permissions apply to its users.
9. Compare identity-based policies and group-based access in terms of flexibility and security.
10. Explain the use of IAM roles in cross-service and cross-account access scenarios.
11. Describe the lifecycle of an IAM role, including its creation, assumption, and revocation.
12. Illustrate the steps to configure an IAM role for an EC2 instance to access S3 securely.
13. Discuss IAM best practices that enhance security in a multi-user AWS environment.
14. Explain how access keys, MFA, and policy conditions contribute to secure IAM management.In AWS Shared Responsibility Model, list and explain any five responsibilities handled

[10 marks]

15. A startup company is planning to launch a global e-commerce website. They expect customers from different continents and want low latency, high availability, and minimal downtime.

    Explain how AWS Global Infrastructure can help meet these requirements. Suggest specific AWS services/features (Regions, AZs, Edge Locations, CloudFront, etc.) that the company should use.

16. An educational institution is moving its student portal to AWS. The IT department is concerned about security, compliance, and maintenance responsibilities.

    Using the AWS Shared Responsibility Model, explain which tasks will be handled by AWS and which must be handled by the institution. Give examples for both security of the cloud and security in the cloud.

17. Describe the process of creating and managing IAM users and groups, and explain how policies can be used to control their permissions with suitable examples.
18. Compare IAM users, groups, and policies in terms of their purpose, scope, and best practices for assigning permissions in a large organization.
19. Explain the concept of IAM roles and illustrate their use in scenarios such as granting temporary access to applications, services, or users across AWS accounts.
20. Discuss at least five IAM best practices recommended by AWS and explain how each helps in improving security and access control.
21. Explain how AWS IAM supports cross-account access using roles, and describe a scenario where this feature is essential in an enterprise cloud architecture.

UNIT - II

[3 Marks]

22. Why do you require elastic load balancing?
23. List various types of storage services available in AWS?
24. Difference between Amazon S3 and S3 Glacier storage service
25. Compare Block storage and Object Storage
26. List out few policies for S3 bucket
27. How Amazon EFS works?
28. Highlight key features of Amazon EC2.
29. State any three EC2 instance families and their primary use cases.
30. What is the purpose of an Elastic IP in EC2?
31. List the four main EC2 pricing models and explain.
32. What is the purpose of an Elastic IP in EC2?
33. Mention any three benefits and key component of AWS Auto Scaling.
34. Write the meaning of “serverless compute” in AWS.

[5 Marks]

35. Discuss the features of Elastic Load Balancing
36. Discuss the various versions of Amazon S3 Services
37. Differentiate Amazon EBS and EFS
38. List out the advantage of using Amazon glacier
39. Compare the pricing model across the storage service
40. List out advantage of using Amazon S3 bucket.
41. Identify the best storage service for handling the live cricket streaming data and mention its illustration.
42. Discuss the feature and pricing strategy of EBS storage
43. Explain the steps for EFS implementation
44. Discuss the common scenarios where Amazon S3 can be used.

45. Explain the differences between On-Demand Instances, Reserved Instances, and Spot Instances.
46. Describe the characteristics and use cases of Compute Optimized instances.
47. Explain the concept of Accelerated Computing instances with examples.
48. Draw and explain the EC2 instance lifecycle.
49. Describe the role of AWS Fargate in serverless container execution.
50. Explain the instance family naming convention in AWS EC2 (prefixes and suffixes).

[10 Marks]

1. "MediaStream" is a growing digital media company with a library of millions of high resolution images and videos. The company faces several critical challenges with its traditional on-premise storage solution:
    a. Scalability Limitations: Their storage servers are constantly running out of space, requiring frequent and expensive hardware upgrades. This manual scaling process is inefficient and cannot keep up with the exponential growth of new content.
    b. High Costs: Maintaining and powering on-premise storage is expensive. They also face significant costs for off-site backups to ensure data durability.
    c. Lack of Durability and Reliability: The risk of data loss due to hardware failure is a constant threat. A single server crash could lead to the permanent loss of valuable media assets.
    d. Poor Global Performance: Serving high-resolution content to a global audience from a single data center results in high latency, slow load times, and a poor user experience for customers in different geographical regions.
    e. Complex Management: The IT team spends significant time managing file permissions, backups, and data migration, taking away from more strategic tasks.

MediaStream decides to migrate its entire media library to any one Amazon Storage Service that should have Industry-leading scalability, data availability, security, and performance. Identify the correct storage service and justify with its features, pros and pricing strategy

2. CodeStream's development and data science teams faced several challenges with their traditional on-premise shared storage:
    a. Fixed Capacity: Their Network File System (NFS) server had a fixed storage capacity. As the teams' projects and datasets grew, they constantly had to purchase and configure new hardware, a time-consuming and expensive process.

b. Performance Bottlenecks: During peak usage, multiple developers or data analysts accessing the same files would cause performance degradation and slow down their workflows.
c. Single Point of Failure: The on-premise NFS server was a single point of failure. If the server went down, both teams would lose access to all their shared data, halting work and impacting project deadlines.
d. Complex Management: The IT team spent a significant amount of time on maintenance, patching, backups, and managing file permissions for the shared storage server.

To solve these problems, CodeStream migrated its shared file storage to Amazon Y. Y provides a simple, scalable, and elastic NFS file system that can be shared across multiple Amazon EC2 instances. Discuss the implementation steps and illustration of Y.

3. "WebStream," a company that provides a content management system (CMS), needs to ensure its platform is highly available and resilient to failure. Their current architecture, which relies on a single web server and an attached storage volume in one data center, has several critical weaknesses:
    a. Single Point of Failure: If the single Availability Zone where their infrastructure resides experiences an outage, the entire CMS platform becomes unavailable to all customers, leading to a loss of service and revenue.
    b. Scalability Issues: The single server cannot handle a sudden surge in user traffic. While they can scale vertically (use a bigger server), this is a temporary and expensive solution.
    c. Manual Data Synchronization: To achieve a form of redundancy, they would have to manually synchronize data between servers in different locations, a complex and error-prone process.

To overcome these challenges, WebStream re-architects its platform using a high-availability, multi-Availability Zone design on AWS. The core of this new architecture is an Amazon X which serves as a single, shared storage repository for all application servers. Discuss the system architecture of the above scenario by identifying X along with its working mechanism.

4. ShopNow" is a rapidly growing online retail company. Their e-commerce website is hosted on a single server, which worked well initially. However, the company faces several critical challenges:
    a. Traffic Spikes: During major sales events (e.g., Black Friday, flash sales), the number of concurrent users can spike from a few hundred to tens of thousands in minutes. The single server frequently crashes under this load, causing downtime and lost sales.
    b. Single Point of Failure: If the server fails for any reason (hardware malfunction, software error), the entire website becomes unavailable. This poses a significant risk to the business and its reputation.

c. Manual Scaling: The IT team has to manually provision and configure new servers in anticipation of major events. This process is time-consuming, prone to errors, and inefficient, as the extra servers sit idle during off-peak hours.
d. Poor Performance: Even when not at peak capacity, the server's response time is inconsistent, leading to a poor user experience and high bounce rates.

To address these issues, ShopNow decides to migrate its website to a cloud based infrastructure and implement X. Identify X and implement the solution that has following components like Multiple Web Servers, X, Auto Scaling, Health Checks with the configuration steps.

5. Discuss the different EC2 instance types in detail (General Purpose, Compute Optimized, Accelerated Computing, Memory Optimized, and Storage Optimized) with examples and use cases.
6. Explain the working of AWS Auto Scaling with EC2, including scaling policies and integration with load balancers.
7. Describe the various EC2 pricing models in detail along with advantages, disadvantages, and suitable scenarios
8. With a neat diagram, explain the complete process of launching an EC2 instance including AMI selection, instance type, storage, network, security groups, and key pairs.
9. Case Study: An organization needs to run high-performance computing for molecular dynamics simulations while minimizing cost. Suggest suitable EC2 instance types and pricing models, and justify your recommendation.
10. A company's web application faces fluctuating traffic throughout the day. Suggest an AWS compute service plan using EC2 and Auto Scaling, justifying your choice

UNIT - III

[3 Marks]

1. What is Amazon VPC?
2. Define a subnet in the context of VPC.
3. What is the difference between a public and a private subnet?
4. Which AWS service allows you to create isolated networks within the AWS cloud?
5. Name any two components of a VPC.
6. What is a default subnet in a default VPC?
7. What is a route table in AWS VPC?
8. What is the purpose of a security group?
9. Define VPC Peering.
10. State one key benefit of AWS Direct Connect.
11. What is Amazon CloudFront used for?

[5 Marks]

12. Explain the purpose of an Internet Gateway in a VPC.
13. Differentiate between default VPC and custom VPC in AWS.
14. Why do we use subnets within a VPC?
15. What are the key differences between a Network ACL and a Security Group?
16. How does a Route Table help manage traffic within a VPC?
17. Identify the difference between a public subnet, a private subnet, and a VPN-Only Subnet.
18. Discuss the steps to create a subnet in AWS using the Management Console or CLI.
19. Describe subnet segmentation for a -tier architecture (Web, App, DB).
20. What are the steps to establish VPC Peering between two VPCs?
21. Describe how route tables help in directing traffic within a VPC.
22. Describe the working of Amazon CloudFront with an S bucket origin.

[10 Marks]

1. Explain the architecture and components of an Amazon VPC. Describe how you would set up a VPC with public and private subnets, an Internet Gateway, and a NAT Gateway for secure access
2. Discuss the role of subnets in AWS VPC design. Include details about subnet sizing (CIDR), availability zones, routing, and security controls.
3. You have launched two EC2 instances — one in a public subnet and another in a private subnet. The instance in the public subnet has a public IP and works fine, but the one in the private subnet cannot access the internet.
    a. Identify the issue.

What solution would you propose to allow internet access from the private subnet?

4. Explain Amazon CloudFront architecture in detail, including edge locations, origin, cache behaviours, and how it integrates with AWS services like S3 or EC2.
5. Explain the lifecycle of a request from a user to a web application hosted on AWS with CloudFront, ALB, EC2, and a database in a private subnet.
6. Design a secure three-tier web application architecture using VPC. Include web application and database tiers using subnets, and describe how traffic is controlled between them.
7. Compare and contrast Security Groups and Network ACLs in Amazon VPC. Provide use-cases where each is suitable.
8. You are tasked with deploying a multi-AZ high-availability architecture using VPC. Explain the networking setup and how traffic distribution, failover, and security

would be handled.

UNIT - IV

[3 Marks]

1. List any three database engines supported by Amazon RDS.
2. Illustrate two AWS managed database services apart from Amazon RDS.
3. Explain the key benefits of using Amazon RDS over self-managed databases.
4. Describe the backup and restore options available in Amazon RDS.
5. Mention the advantages of Multi-AZ deployment in Amazon RDS.
6. What is the primary purpose of an Amazon RDS Read Replica?
7. Name two differences between Amazon Aurora and standard MySQL/PostgreSQL
8. RDS engines.
9. What type of database is Amazon DynamoDB?
10. What event information does DynamoDB Streams capture?

[5 Marks]

1. Explain the key benefits of using Amazon RDS over self-managed databases.
2. Differentiate between Single-AZ and Multi-AZ deployments in Amazon RDS.
3. Describe the backup and restore options available in Amazon RDS.
4. Explain the concept of Read Replicas in RDS and how they differ from Multi-AZ
5. deployments.
6. Briefly illustrate the steps to create an RDS instance in AWS?
7. Explain how RDS Read Replicas help in improving database performance and
8. availability.
9. Explain how Amazon Aurora achieves high availability and fault tolerance.
10. Compare DynamoDB's provisioned capacity and on-demand capacity modes.
11. Explain how DynamoDB Streams can be used with AWS Lambda for real-time data
12. processing.

[10 Marks]

1. Discuss the architecture and benefits of Amazon RDS Multi-AZ deployments. Include how failover works.
2. Compare Amazon RDS with Amazon Aurora in terms of performance, scalability, and availability.
3. Explain how Amazon RDS provides high availability, fault tolerance, and automated maintenance. Provide real-world examples.
4. Design a high-availability database solution using Amazon RDS for an e-commerce application. Include considerations like failover, backups, and scaling.

5. Evaluate the pros and cons of using Amazon RDS versus deploying your own database on EC2 instances.
6. Your e-commerce application experiences heavy read traffic during flash sales.
7. Propose an architecture using RDS Read Replicas to handle the load, and explain how you would minimize replication lag impact on user experience.
8. Given a requirement for a database that must sustain millions of requests per minute with automatic scaling and high fault tolerance, justify why Amazon Aurora might be chosen over MySQL RDS. Support your answer with architectural reasoning.
9. You are designing a gaming leaderboard system on DynamoDB that must return top scores quickly while handling sudden spikes in writes. Explain your table design, partition key selection, and capacity mode choice.
10. A logistics company wants to track every change in package status in real time and send updates to a notification service. Design a solution using DynamoDB Streams and AWS Lambda, explaining ordering guarantees and failure handling.

UNIT - V

[3 Marks]

11. Define AWS Management Tools and name any four services included in this category.
12. What is Amazon CloudWatch and what are its two primary purposes?
13. Define AWS CloudTrail and state one difference between CloudTrail and CloudWatch.
14. What is AWS Config used for in compliance monitoring?
15. Name two types of automation documents (runbooks) used in AWS Systems Manager.
16. Mention any three AWS Cost Management tools.
17. What is a CloudWatch Metric? Give an example.
18. State the retention period of CloudTrail logs by default.
19. What is the purpose of AWS Budgets in cost management?
20. Define Compliance Packages in AWS Config.
21. Define the AWS Free Tier and its three types of offers.
22. What is the difference between the 12-Month Free Tier and the Always Free Tier in AWS?
23. State two use cases of AWS Budgets.
24. Define AWS Trusted Advisor and list any three categories it checks.
25. What is the difference between the AWS Basic Support plan and the Developer Support plan?
26. List two benefits of enabling consolidated billing in AWS Organizations.
27. Mention two differences between AWS Cost Explorer and AWS Budgets.

[5 Marks]

1. Explain the difference between CloudWatch Logs, Metrics, and Events with examples.
2. How does AWS CloudTrail help in security auditing? Give two examples.
3. Describe the main components of AWS Systems Manager and their purpose.
4. Explain the working of AWS Config in tracking configuration changes with an example.
5. Differentiate between AWS Cost Explorer and AWS Budgets.
6. Describe a scenario where you would use AWS Systems Manager Automation instead of manual intervention.
7. Explain resource-level permissions in AWS Systems Manager with an example.
8. What is the role of CloudWatch Alarms? How are they triggered?
9. Explain how Cost Anomaly Detection works in AWS Cost Management.
10. Compare Management Tools in AWS and traditional on-premises management tools.
11. Explain the three main types of AWS Free Tier offers with suitable examples.
12. A startup wants to track monthly EC2 and S3 usage costs. Explain how AWS Budgets can help them.
13. Compare AWS Trusted Advisor free checks vs full checks (Business/Enterprise Support).
14. Describe how a user can set up alerts for exceeding a budget threshold in AWS.
15. You have an AWS account under the Free Tier but still received a bill. Explain two possible reasons why.
16. Compare the role of AWS Billing console and AWS Cost Explorer in managing expenses.
17. A company wants to optimize unused EC2 instances. Explain how AWS Trusted Advisor recommendations can help.

[10 Marks]

1. Your organization suspects a security breach. Describe how you would use CloudTrail, CloudWatch, and AWS Config together to investigate and resolve the issue.
2. You are tasked to reduce AWS monthly bills. Explain how you would use AWS Cost Explorer, AWS Budgets, and Cost Anomaly Detection to achieve this goal, including example reports or dashboards.
3. Compare and contrast AWS CloudWatch and AWS CloudTrail in terms of purpose, data collected, retention, and integration with other services.
4. Explain in detail how AWS Systems Manager Patch Manager works. Include how it schedules, executes, and verifies patching.

5. A compliance audit requires proof of configuration history for all EC2 instances in the last 6 months. Explain the steps using AWS Config and AWS Systems Manager Inventory.
6. Discuss the end-to-end process of creating and monitoring a custom CloudWatch metric for application latency, including alarm setup and automated remediation.
7. Compare AWS Management Tools suite with equivalent tools from Azure or Google Cloud in terms of monitoring, auditing, and cost tracking.
8. Explain the integration flow between AWS CloudWatch, AWS Lambda, and AWS Systems Manager Automation in auto-remediation of EC2 instance failures.
9. Your team needs automated OS updates across 200 EC2 instances without downtime. Describe how you would achieve this using Systems Manager Maintenance Windows and Patch Manager.
10. Provide a detailed explanation of AWS Config Rules, their types (managed vs. custom), and how they help maintain compliance in regulated industries.
11. A small business uses AWS Free Tier for hosting a web application. After 6 months, they notice increasing costs.
    - Identify three possible causes for the increased billing.
    - Suggest three AWS tools/features they can use to control and optimize costs.
12. Explain in detail how AWS Budgets can be used to manage and forecast costs for a multi-account AWS Organization.
13. Compare and contrast AWS Trusted Advisor with AWS Cost Explorer in terms of purpose, scope, and use cases.
14. A project team has a strict monthly budget of $500 for AWS services. Create a step-by-step plan to:
    - Set the budget in AWS Budgets
    - Receive alerts at 80% usage
    - Take corrective actions based on Trusted Advisor recommendations.
15. Discuss AWS Free Tier limitations and best practices for avoiding unexpected charges, with real-world examples.

UNIT - VI

[3 Marks]

1. Define the AWS Shared Responsibility Model using AWS's official definition. List two customer responsibilities for Amazon RDS.
2. What are the three types of customer master keys (CMKs) in AWS KMS? Briefly describe each.

3. Name three AWS services that natively integrate with KMS for encryption.
4. What is the default key rotation period for AWS-managed KMS keys? Can it be modified?
5. List two compliance programs where AWS KMS is explicitly mentioned as a compliant service.
6. Define the AWS Shared Responsibility Model and list two customer responsibilities for EC2 instances.
7. What is the primary purpose of AWS KMS? Name two AWS services that integrate with it.
8. List three security compliance standards that AWS KMS supports.
9. Differentiate between AWS-managed keys and customer-managed keys in KMS.
10. What is the significance of FIPS 140-2 validation in AWS KMS?
11. Define AWS WAF and mention its primary purpose.
12. What is the difference between rate-based rules and regular rules in AWS WAF?
13. Name three common attack types AWS WAF can help mitigate.
14. What is AWS Shield Standard and how is it different from AWS Shield Advanced in terms of cost?
15. List three benefits of implementing AWS security best practices in cloud architecture.
16. What is a Web ACL in AWS WAF?
17. State two main differences between AWS WAF and AWS Shield.
18. Mention two AWS services that integrate directly with AWS WAF.
19. What is the purpose of AWS Well-Architected Framework – Security Pillar?
20. List two common metrics available in AWS WAF for monitoring.

[5 Marks]

1. Design a KMS key policy that:
    i) Allows IAM users in Account A to encrypt/decrypt data
    ii) Denies all actions if the request originates from outside the VPC vpc-123456.
2. Explain how KMS envelope encryption works with S3. Include the roles of Data Key and CMK.
3. A company must audit KMS key usage for compliance. Outline steps using AWS CloudTrail and Amazon Athena.
4. How does AWS KMS differ from Secrets Manager for managing database credentials? Provide two use cases for each.
5. A financial institution must encrypt S3 data using customer-managed KMS keys.
   Design an IAM policy that:
    i) allows only the "Audit" IAM role to use the key
    ii) denies deletion of the key
6. Explain how AWS KMS key rotation works. Compare automatic vs. manual rotation for compliance-sensitive workloads

7. Assume a company uses CloudHSM for cryptographic operations. Outline three scenarios where CloudHSM is mandatory over KMS
8. A multi-account AWS environment needs to share encrypted S3 buckets. Design a solution using KMS key policies and cross-account access
9. Compare KMS and CloudHSM using AWS's official comparison criteria:
    i) Hardware isolation - multi-tenant vs. single-tenant
    ii) Key management control AWS vs. customer
10. Contrast SSE-KMS vs. SSE-S3 for S3 encryption:
    i) Audit capability -CloudTrail logs)
    ii) Permission model -IAM vs. KMS key policies
11. Compare KMS and CloudHSM in terms of:
    i) Tenancy -shared vs. dedicated hardware)
    ii) Compliance requirements
12. Contrast server-side encryption with KMS (SSE-KMS) and client-side encryption for S3:
    i) Key management responsibility.
    ii) Use cases -static data vs. high-security workloads
13. Explain the architecture of AWS WAF and describe how a request is filtered.
14. Compare AWS Shield Standard and AWS Shield Advanced in terms of features, cost, and target use case.
15. How does AWS WAF integrate with Amazon CloudFront to protect web applications? Provide an example.
16. List and explain three AWS Security Best Practices for protecting workloads from unauthorized access.
17. Discuss the role of Managed Rule Groups in AWS WAF. Give two use case examples.
18. Explain rate-based rules in AWS WAF with an example of when they might be applied.
19. Describe how AWS Shield Advanced provides DDoS attack protection and response.
20. What are the five design principles of the AWS Well-Architected Framework's Security Pillar?
21. Compare AWS Security Groups and Network ACLs in terms of AWS security best practices.
22. How does logging in AWS WAF work and why is it important?

[10 Marks]

1. Financial Institution Scenario:PCI-DSS compliance for cardholder data with FIPS 140-2 Level 3 validation.
    a. Justify using CloudHSM over KMS citing AWS documentation.
    b. Design a key hierarchy using KMS CMKs and data keys.
    c. How would AWS Config monitor non-compliant KMS key configurations?

2. Multi-Region SaaS Provider Scenario:Encrypt customer data with regional isolation using KMS.
    a. Explain KMS multi-region keys and their replication behavior.
    b. Design a cross-account access pattern for KMS keys using key policies.
    c. How would AWS Organizations SCPs enforce KMS encryption for all EBS volumes?
3) Healthcare Compliance Scenario: HIPAA-compliant encryption for patient data in transit and at rest.
    a) Justify using KMS with AWS Certificate Manager for TLS certificates.
    b) Design a data encryption flow for EBS volumes and RDS using KMS.
    c) How would CloudTrail audit KMS key usage?
4) Financial Services Scenario: PCI-DSS compliance for payment processing with strict key control.
    a) Explain why CloudHSM is required for cryptographic operations.
    b) Design a key policy to restrict access to the security team + audit logs.
    c) How would AWS Organizations SCPs enforce KMS encryption for all S3 buckets?
5) An e-commerce company is facing frequent SQL injection and XSS attacks on its application hosted on AWS. Explain how AWS WAF can be configured to mitigate these threats. Include details on rule creation, managed rules, and monitoring.
6) A financial services application must be protected from large-scale DDoS attacks and needs 24/7 monitoring with AWS SOC support. Compare AWS Shield Standard and Advanced, and recommend which one should be used, justifying your choice.
7) Explain step-by-step how to secure a public-facing web application using AWS WAF, AWS Shield Advanced, CloudFront, and AWS Security Best Practices. Include architectural reasoning.
8) Compare the security benefits and operational differences of using AWS WAF with CloudFront vs. AWS WAF with Application Load Balancer (ALB) in protecting against OWASP Top 10 threats.
9) A healthcare SaaS platform must comply with HIPAA regulations and ensure minimal downtime during attacks. Propose a comprehensive AWS security strategy using AWS WAF, AWS Shield, AWS Security Hub, and other best practices.
10) Discuss the Security Pillar of AWS Well-Architected Framework in detail, explaining how AWS WAF and AWS Shield align with its principles. Provide practical examples.
11) Evaluate the cost-benefit trade-off of implementing AWS Shield Advanced for a small business with occasional traffic spikes versus an enterprise with mission-critical workloads.
12) Describe in detail how to configure custom rules in AWS WAF to block malicious IP ranges, limit request rates, and inspect request bodies. Provide a step-by-step configuration plan.
13) Your startup plans to launch a mobile game globally. Describe the security architecture you would implement using AWS WAF, AWS Shield, AWS IAM, and CloudFront to protect against both application layer and network layer attacks.
14) Compare AWS WAF and AWS Firewall Manager in terms of centralized management, cost, and scalability, and explain when to use each.

UNIT - VII

[3 Marks]

1. Explain what is meant by Application Integration in AWS. List any three AWS services used for integrating applications.
2. Briefly describe the purpose of two Application Integration services.
3. List any three key features of Amazon Simple Queue Service (SQS).
4. What is Amazon Simple Notification Service (SNS), and what are its primary use cases?
5. What is Amazon Simple Workflow Service (SWF), and what is its primary purpose?
6. What are typical security considerations when designing SWF workflows in AWS?
7. How does Amazon SWF coordinate complex workflow steps in real scenarios?
8. What is AWS Step Functions, and what are its primary benefits?
9. What are the main components and states used in AWS Step Functions?
10. What are common use cases for choosing between Standard and Express workflows?
11. What is the AWS Well-Architected Framework, and what are its primary goals?
12. A startup is building a new application and has a very tight budget and a small development team. They have decided to use an Amazon RDS database. Their architects are debating whether to use a Multi-AZ deployment from the start or to implement it later. From a design principles perspective, why would it be a better long-term strategy to prioritize loose coupling and statelessness in their application tier over immediate Multi-AZ deployment for the database?
13. Propose a scaling strategy that is more effective and cost-efficient than a simple CPU-based Auto Scaling policy. Justify your choice by explaining how it specifically addresses the nature of the workload.
14. An application's data is stored on an Amazon EBS volume attached to a single EC2 instance. The company needs to ensure the data is durable and can be recovered quickly in the event of an EC2 instance failure. Besides taking regular snapshots, what is the most straightforward and fundamental change you could make to the data's storage configuration to improve its fault tolerance? Explain how this change works.
15. A team is building an application that needs to securely write data to an Amazon S3 bucket. They are considering embedding the IAM user access keys and secret keys directly into the application's source code. From a security best practices standpoint, why is this an extremely bad idea, and what is the AWS-recommended, more secure alternative to provide the application with the necessary permissions?
16. A batch processing job runs daily for approximately 8 hours, processing a consistent workload. The company is currently using On-Demand EC2 instances for this job. What specific change to the EC2 pricing model and instance type would you recommend to significantly reduce costs? Justify your recommendation by explaining how this model is uniquely suited to this type of predictable, long-running workload.

17. Compare and contrast the use of Amazon EC2 Auto Scaling with AWS Lambda for handling a web application's fluctuating traffic. Analyze the trade-offs between these two services in terms of operational complexity, cost-effectiveness for a bursty workload, and the granularity of scaling.
18. You are a solutions architect designing a new database for a critical application. You have to choose between a Multi-AZ Amazon RDS deployment and a multi-master Amazon Aurora Global Database. Compare these two options, focusing on their respective strengths and weaknesses in achieving high availability, fault tolerance, and disaster recovery
19. Compare and contrast AWS Identity and Access Management (IAM) Roles and IAM Users for an EC2-based application that needs to access other AWS services. Discuss the security implications of each approach and explain why one is a more secure, recommended best practice for this scenario
20. A company is looking to optimize costs for its compute resources. They have a workload that can be interrupted and a critical workload that cannot. Compare and contrast the use of EC2 Spot Instances and EC2 Savings Plans. Explain how you would use a combination of both to achieve a significant cost reduction while ensuring the critical workload's availability
21. Compare and contrast a tightly coupled monolithic architecture with a loosely coupled microservices architecture. Analyze the impact of each design on a company's ability to innovate, deploy features independently, and achieve fault isolation

[5 Marks]

22. Explain the two types of queues available in Amazon SQS and where these are best used.
23. Give one practical scenario where SQS is especially beneficial. Explain why.
24. Explain the concept of topics and subscriptions in Amazon SNS. How does SNS support different types of endpoints?
25. How does Amazon SNS differ from other messaging services in AWS?
26. How to configure SNS topics for secure message delivery?
27. How to integrate SNS with other AWS services for automated alerting?
28. Explain the key components of Amazon SWF and their roles.
29. Describe the architecture and working of Amazon Simple Workflow Service (SWF).
30. Discuss how SWF manages workflow execution and task coordination, and give an example of a practical use case.
31. How does SWF integrate with other AWS services for scalable application orchestration?
32. Explain the different state types in AWS Step Functions and their roles in a state machine.
33. How does error handling and retries work within AWS Step Functions?
34. List and briefly describe the six pillars of the AWS Well-Architected Framework.
35. Compare Amazon SQS and Amazon SNS in terms of architecture, message delivery patterns.

36. Discuss two scenarios with examples and compare SWF and AWS Step functions.
37. Discuss about the design principle of "Automatically recover from failure" (from the Reliability Pillar)
38. Explain the importance of both scalability and elasticity in cloud computing environments
39. Provide an example of an AWS service that facilitates loose coupling to mitigate failures in distributed systems
40. Outline the customer's responsibilities for "security in the cloud" according to the shared responsibility model
41. Describe two distinct approaches to cost optimisation in AWS cloud architectures
42. Discuss how the design principle of "Automatically recover from failure" (from the Reliability Pillar) and "Use managed services" (from the Operational Excellence Pillar) contribute to a well-architected system.
43. Explain the importance of both scalability and elasticity in cloud computing environments. Describe how AWS enables organisations to adjust resources dynamically
44. Explain how architecting a workload using a service-oriented architecture (SOA) or a microservices architecture can enhance reliability and resilience
45. Outline the customer's responsibilities for "security in the cloud" according to the AWS architecture model. Additionally, explain the importance of "implementing a strong identity foundation" as a key design principle in AWS security
46. Describe two distinct approaches to cost optimisation in AWS cloud architectures. Your explanation should cover how these approaches help to reduce overall expenditure and maximise business value.
47. Describe how specific AWS Application Integration services, such as Amazon SQS and Amazon SNS would be utilised to facilitate loose coupling and manage the required asynchronous message handling. In addition, discuss how you would approach the orchestration of complex workflows within this distributed system
48. Detail the steps and specific AWS services they would leverage to define their infrastructure, manage application deployments, and handle routine operational tasks as code. Furthermore, describe how using managed services for complex technologies (e.g., NoSQL databases) would free up their team's focus and contribute to both operational and performance goals
49. A rapidly growing e-commerce company needs to ensure its new cloud-native application can handle unpredictable demand spikes and growing workloads while optimising resource usage. Explain the implementation steps for designing this application to achieve dynamic scalability and elasticity using AWS capabilities
50. Explain how the principle of "Automatically recover from failure" would be applied, including distributing resources across multiple Availability Zones (AZs) and potentially AWS Regions to avoid single points of failure. Additionally, describe how adopting a Service-Oriented Architecture (SOA) or microservices architecture contributes to decoupling and resilience in this distributed system

51. An enterprise aims to continuously optimize its cloud spending after migrating several workloads to AWS. Explain the actionable steps and ongoing processes they should implement to drive Cost Optimization effectively, beyond initial "lift and shift" savings.
52. Compare and contrast the traditional on-premises data center design principles with the cloud-native design principles advocated by AWS (e.g., disposable resources, loose coupling, designing for failure). Discuss how these differing philosophies impact architectural choices and operational models in the cloud.
53. Differentiate between "scalability" and "elasticity" in the context of AWS cloud architectures. Explain how AWS services like Auto Scaling Groups and Serverless compute (e.g., AWS Lambda) address both concepts, highlighting their primary distinctions in achieving adaptive capacity.
54. While often used interchangeably, High Availability and Fault Tolerance have distinct implications in cloud design. Compare and contrast these two concepts, providing examples of how AWS services (e.g., Multi-AZ deployments vs. cross-Region disaster recovery or services like S3) contribute to achieving each, and discuss when one might be prioritized over the other
55. Compare and contrast the shared responsibility model in AWS with a traditional on-premises security model. Discuss how the distribution of security responsibilities impacts an organization's approach to securing their data and applications on AWS versus in their own data centers, focusing on both advantages and challenges
56. Compare and contrast the effectiveness of "right-sizing" existing resources versus leveraging "reserved instances" or "Savings Plans" as cost optimization strategies in AWS. Discuss scenarios where each strategy provides a more significant cost benefit and how they can be combined for comprehensive cost savings

[10 Marks]

57. HelloSALES runs an e-commerce website that experiences unpredictable traffic spikes, especially during special sales events. During these spikes, order requests can flood the backend processing systems. It often overwhelms the servers responsible for payment processing and inventory updates, leading to delayed or lost orders. Explain how and why an Amazon cloud service can be implemented to safeguard order processing reliability and outline the architectural approach.
58. Discuss the working principle, main features, different types of queues, key operations in SQS.
59. Describe Amazon SNS in detail, including its architecture, message delivery mechanisms, supported protocols, and common use cases. Explain how it ensures message reliability and how you can secure SNS topics.
60. In a multi-component web application, different subsystems need to receive notifications whenever a user updates their profile, places an order, or changes subscription status. These

notifications should be sent to various endpoints like email for customer service, SMS for urgent alerts, and an SQS queue for further asynchronous processing. Explain how you would use any Amazon service to design this notification system. Describe the workflow and benefits of using that product.

61. A multinational company wants to automate a complex business process involving multiple tasks that need to be executed sequentially and in parallel, with fault tolerance and retry logic. The tasks include data validation, processing, and notification. How would you use Amazon services to design and manage this workflow?
62. RollingMedia needs to process video files uploaded by users. The processing pipeline includes tasks like transcoding, metadata extraction, and thumbnail generation, each performed by different distributed components. Which Amazon service be used to coordinate this pipeline to ensure tasks are executed in the correct order with monitoring and error handling? How?
63. An e-commerce platform's order fulfillment process requires multiple long-running tasks such as payment authorization, inventory check, and shipment scheduling. The tasks may take minutes or hours, and you want to ensure the system is resilient to worker failures and can provide execution status to users. How would you implement this using Amazon services?
64. Discuss AWS Step Functions in detail. Describe its architecture, key components, state machine concepts, main features, and provide use cases where Step Functions are especially beneficial.
65. Highlighting key design principles of AWS Well Architected Framework explain why these are important for cloud architectures.
66. LethalCorp company needs to build a video processing pipeline that involves multiple steps. It includes uploading a video, transcoding it into multiple formats, extracting metadata, generating thumbnails, and finally notifying users when processing completes. The pipeline should handle tasks in sequence and in parallel where appropriate, retry on errors, and be easily monitored. How would you design this workflow using AWS services? Describe the components and benefits of this approach.
67. Compare Amazon SWF and AWS Step Functions in terms of service architecture, workflow orchestration capabilities.
68. Explain how AWS cloud design principles serve as a guide for architectural decisions and help identify areas for improvement in a system's architecture. Discuss, in detail, how adherence to the framework's six pillars along with general design principles, collectively contributes to the successful design, operation, and evolution of cloud workloads.
69. Scalability and elasticity are fundamental characteristics of cloud computing, enabling systems to dynamically adjust resources to meet fluctuating demand and handle growing workloads. Explain how these concepts are realised in AWS environments, elaborating on how organisations can "stop guessing capacity needs".
70. Detail how service-oriented architecture (SOA) or microservices architecture promote loose coupling and independent components to enhance reliability and resilience in

distributed systems. Provide examples of how AWS services and architectural patterns, such as deploying across multiple Availability Zones, support these objectives

71. Elucidate the distinct responsibilities of both AWS ("security of the cloud") and the customer ("security in the cloud") within a shared responsibility and data protection model. Discuss the significance of "implementing a strong identity foundation" as a core design principle for security
72. Detail the design principle of "Implement Cloud Financial Management", explaining its importance for financial success and business value realisation. Discuss how adopting a consumption model (pay-as-you-go) fundamentally alters cost structures compared to traditional IT.
73. A legacy monolithic application, currently running on-premises, needs to be re-platformed onto AWS. The application is critical for business operations and cannot afford significant downtime. Describe the core AWS design principles you would follow to guide this migration. Outline a high-level, step-by-step migration plan, justifying how each step adheres to a specific design principle.
74. An e-commerce website experiences predictable traffic surges during holidays and unpredictable spikes during flash sales. Design a scalable and elastic architecture for the application layer. Name the specific AWS services you would use, and explain how they work together to automatically handle fluctuating traffic while optimizing for cost. Provide a justification for choosing a specific scaling metric (e.g., CPU Utilization, Request Count) for your solution
75. You are tasked with designing a highly available and fault-tolerant architecture for a critical web application that serves global users. The application consists of a stateless web tier, a stateful database, and a caching layer. Describe how you would implement high availability for each of these three components. Explain the difference between high availability and disaster recovery, and propose a strategy to ensure business continuity in the event of a regional outage.
76. A financial services company needs to host a new application on AWS that handles sensitive customer data. This requires a strong security posture covering multiple layers. Describe the layered security model you would implement. Explain how you would secure the following:
    a. Network access (VPC and subnets)
    b. Application access (IAM roles and policies)
    c. Data at rest and in transit (Encryption methods)
    d. Logging and Monitoring (Audit trails)
77. A startup with a limited budget is launching a new video streaming service. The service is expected to have a low initial user base but grow rapidly over time. As a solutions architect, what three distinct cost optimization strategies would you recommend to the startup? For each strategy, name the AWS services or features involved and explain how they would reduce costs from day one without compromising future scalability

78. Discuss how adherence to general cloud design principles, such as "stop guessing your capacity needs", "use managed services", and "perform operations as code", fundamentally changes the architectural process and outcomes compared to conventional on-premises planning
79. Explain how cloud capabilities, including auto-scaling, on-demand provisioning, and leveraging different pricing models enable dynamic resource adjustment and cost efficiency. Discuss why these are difficult or impossible to achieve with fixed, pre-provisioned traditional hardware resources, thus illustrating how the cloud helps organisations "stop guessing capacity needs
80. Contrast the approaches to achieving High Availability (HA) and Fault Tolerance in modern distributed cloud systems, like those built on AWS, with traditional on-premises data center strategies. Discuss how cloud design principles, such as deploying workloads across multiple Availability Zones (AZs) and AWS Regions, coupled with the adoption of Service-Oriented Architecture (SOA) or microservices, inherently enhance resilience and automated recovery from failures. Compare this to the challenges and common limitations of ensuring business continuity and disaster recovery in single-location, tightly coupled traditional IT infrastructures
81. Discuss the fundamental differences in security responsibility and implementation between an AWS cloud environment and a traditional on-premises data center, as outlined by the AWS Shared Responsibility Model. Explain how cloud design principles like "implementing a strong identity foundation" (including least privilege and centralized identity management), "maintaining traceability" through real-time monitoring and auditing, and adopting AWS-managed services contribute to a distinct and often superior security posture in the cloud when compared to conventional IT security models.
82. Analyse the significant differences in cost structure and optimisation methodologies between deploying and operating IT workloads in the AWS cloud versus a traditional on-premises data center. Compare how the cloud's "consumption model" (pay-as-you-go), along with specific design principles like "Implement Cloud Financial Management", "cost-effective resource selection" (including right-sizing and various pricing models), and "managing demand and supply resources", enables organisations to achieve financial agility and reduce overall expenditure in ways that are distinct from, and often superior to, traditional IT capital expenditure planning.

UNIT - VIII

[3 Marks]

1. Define AWS Snowball and its core function.
2. List three security features available in Snow Family devices.

3. Identify the use case scenarios best suited for AWS Snowmobile.
4. Describe the types of data transfer challenges that AWS Snow Family solves.
5. Recall the difference between Snowball and Snowball Edge in terms of processing capability.
6. Define hybrid cloud architecture in AWS.
7. List any three benefits of using hybrid cloud architecture.
8. What is AWS Direct Connect used for?
9. Mention two scenarios where hybrid architecture is preferred.
10. What is AWS Database Migration Service (DMS)?
11. State any two databases supported by AWS DMS.
12. What is the difference between homogeneous and heterogeneous database migrations in DMS?
13. Differentiate between full load and change data capture (CDC) migration approaches in DMS.
14. List and explain the major steps in migrating an on-premises MySQL database to Amazon RDS using DMS.
15. How does AWS DMS help achieve minimal downtime during database migration?
16. What does AWS Server Migration Service (SMS) migrate?
17. Name the supported operating systems for AWS SMS.
18. How is AWS SMS different from manual VM image uploads?

[5 Marks]

19. Compare AWS Snowball and Snowmobile based on storage size, transport method and use case.
20. Explain how AWS Snowball Edge enables edge computing with local processing.
21. Illustrate the process involved in transferring data using AWS Snowball to an S3 bucket.
22. Summarize how AWS secures data both in transit and at rest in Snowmobile.
23. Classify the Snow Family devices based on data volume, connectivity and local processing features.
24. Explain how a company can ensure secure data transfer between on-premises data centers and AWS cloud in a hybrid architecture.
25. Describe the role of AWS Storage Gateway in hybrid cloud setups.
26. Illustrate with a diagram how AWS supports hybrid architectures for global businesses.
27. Differentiate between full load and change data capture (CDC) migration approaches in DMS.
28. List and explain the major steps in migrating an on-premises MySQL database to Amazon RDS using DMS.
29. How does AWS DMS help achieve minimal downtime during database migration?
30. Explain the workflow of a server migration from on-premises VM to AWS using SMS.

31. Compare the advantages of SMS over other migration tools for lift-and-shift scenarios.
32. Describe the role of AWS SMS automation in large-scale migrations.
33. A startup wants to move its on-premises MySQL database to Amazon RDS using AWS DMS to improve scalability. Describe the key steps involved in this migration process.
34. Explain how AWS Server Migration Service (SMS) can assist a medium-sized business in migrating virtual machines from their on-premises environment to AWS with minimal manual intervention.
35. A company wants to implement a hybrid cloud architecture for their website where customer data stays on-premises for compliance reasons, but the site's traffic handling is offloaded to AWS during peak times. How can AWS support such a setup?
36. Describe how continuous data replication works with AWS Database Migration Service (DMS) and how it helps in minimizing downtime during database migration.
37. Compare AWS DMS and AWS SMS in terms of their migration focus and typical use cases, supporting your answer with examples.

[10 Marks]

1. A healthcare organization needs to transfer 10 PB of patient imaging data from multiple hospital branches to AWS within a short time frame. Recommend a suitable Snow Family service and justify your choice based on security, transport, and efficiency.
2. A remote mining site has no internet connectivity and must process high-resolution geological data before uploading. Select an appropriate Snow service and illustrate the deployment and processing flow.
3. Analyze and contrast Snowball Edge and Snowmobile in terms of physical transport, cost-effectiveness, scalability and ideal industry scenarios.
4. Compare the scalability and security aspects of pure cloud vs hybrid cloud architecture with suitable examples.
5. Analyze the challenges and solutions for integrating legacy on-premises applications with AWS services in a hybrid model.
6. Design a hybrid architecture for a healthcare organization that must comply with data residency regulations.
7. A company is migrating its Oracle database to Amazon RDS for PostgreSQL using DMS. Outline the migration plan, highlighting how DMS handles schema conversion and data validation.
8. Discuss the challenges in migrating large databases using DMS and strategies to overcome them.
9. Evaluate AWS DMS as a tool for continuous data replication in a hybrid environment.
10. Analyze the key differences between AWS SMS and AWS DMS in terms of what they migrate, use cases, and how they operate.

11. Propose a migration strategy for a retail company wants to move hundreds of on-premises servers (including databases and web servers) to AWS using both SMS and DMS.
12. Evaluate the impact of server migrations on business continuity and how SMS helps address these challenges.
13. A financial institution needs to migrate its on-premises Oracle database to Amazon RDS for PostgreSQL with minimal downtime. Explain in detail how AWS Database Migration Service (DMS) can be utilized to accomplish this. Include the migration steps and how data integrity and downtime are managed during the migration.
14. A retail company plans to move its entire on-premises data center—including web servers, application servers, and databases—to AWS. Propose a migration strategy using AWS SMS and AWS DMS that ensures business continuity, scalability, and security. Explain how the hybrid cloud model will support their operations during and after migration.
15. A healthcare provider wants to implement a hybrid cloud architecture where sensitive patient data remains on-premises to comply with regulations, but compute-heavy analytics and application backends are hosted on AWS. Design an architecture to address these requirements and discuss the AWS services involved, including how data synchronization and security are maintained.
16. Analyze the challenges and solutions for migrating a large enterprise MySQL database from on-premises to Amazon RDS using AWS DMS. Include considerations related to network bandwidth, data validation, and performance during and after migration.