Question Bank			
Unit I – Cloud Computing: Introduction			
Sl. No	**Unit**	**Question**	**Options**
1	I	Which of these best defines cloud computing?	a) Local app hosting, b) On-demand network access to shared resources, c) Physical hardware only, d) Webpage hosting only
2	I	What is a key advantage of cloud storage?	a) Enhanced local speed, b) Scalability and remote access, c) Permanent local copies, d) Manual backup only
3	I	Which component manages the integration and flow in a typical cloud architecture?	a) Data center, b) Orchestrator, c) API Gateway, d) Browser
4	I	What is the difference between public and private clouds?	a) Hardware only, b) Ownership and access control, c) Programming language, d) Bandwidth used
5	I	Which event marked the commercial emergence of cloud computing?	a) Email invention, b) Launch of Amazon Web Services, c) Java release, d) FTP protocol
6	I	A disadvantage of public clouds is:	a) Higher scalability, b) Security and shared resources, c) Local cost, d) Physical access
7	I	Which technology primarily enabled the rise of cloud computing?	a) Virtualization, b) DOS, c) CRT monitors, d) Dial-up
8	I	In which model do customers pay for only what they use?	a) Subscription, b) Pay-as-you-go, c) Upfront purchase, d) Open source
9	I	What is cloud elasticity?	a) Changing programming language easily, b) Exporting data, c) Retiring old servers, d) Scaling resources dynamically on demand
10	I	Which is not a core benefit of cloud computing?	a) Agility, b) Resource pooling, c) Manual provisioning only, d) Cost saving
11	I	In cloud storage, what is a "multi-tenancy" characteristic?	a) One user per server, b) Multiple users sharing same infrastructure, c) Dedicated cables, d) No virtualization
12	I	Which layer in cloud architecture is responsible for providing VMs or containers?	a) Application, b) Infrastructure, c) User, d) Data

13	I	Before cloud, what was the major barrier for startups hosting web apps?	a) Bandwidth, b) Programming skills, c) High infrastructure costs, d) Office space
14	I	Cloud allows for resource "pooling". This means:	a) All data in a single place, b) Sharing resources among users dynamically, c) Encrypted apps, d) Isolated servers
15	I	Which is a correct statement about cloud service availability?	a) It is guaranteed for 10% downtime, b) It is typically measured in SLA as uptime percentage, c) It is always manual, d) It never uses failover systems
Unit II – Cloud Deployment & Service Models			
Sl. No	**Unit**	**Question**	**Options**
1	II	Which is a defining feature of public cloud deployment?	a) Isolated infrastructure, b) Shared resources for all clients, c) Only government use, d) Compulsory VPN
2	II	What does "IaaS" stand for?	a) Internet-as-a-Service, b) Infrastructure-as-a-Service, c) Interface-as-a-Service, d) Input-as-a-Service
3	II	Which service model most likely gives you highest user control?	a) SaaS, b) PaaS, c) IaaS, d) DBaaS
4	II	Which layer controls the runtime, middleware, and OS?	a) SaaS, b) IaaS, c) PaaS, d) DaaS
5	II	What is a unique advantage of hybrid cloud deployment?	a) Use only one vendor, b) Data remains entirely private, c) Balance of public/private resource use, d) No security needed
6	II	In a community cloud, resources are:	a) Owned by single org, b) Shared by several orgs. with similar needs, c) Leased to public, d) Not virtualized
7	II	Which is an example of SaaS?	a) Dropbox, b) AWS EC2, c) Kubernetes, d) Docker Hub
8	II	What deployment model is most suitable for handling sensitive government data?	a) Public, b) Hybrid, c) Community, d) Private
9	II	What is the main risk in multi-tenant cloud models?	a) Per-user pricing, b) Data isolation and security, c) Slow networking, d) Lack of storage
10	II	Which model best fits scalable, on-demand application hosting?	a) Traditional server, b) PaaS, c) Desktop as service, d) Local install

11	II	Which attribute is central to SLA in cloud services?	a) Internet speed, b) Service uptime/performance guarantee, c) GUI theme, d) Programming language
12	II	Security in public clouds is majorly handled by:	a) Only client, b) Only cloud provider, c) Both client and provider, d) Government agency
13	II	In terms of control, which model offers least?	a) SaaS, b) IaaS, c) PaaS, d) Hybrid
14	II	Which component is responsible for virtualizing resources for client use?	a) Data center operator, b) Hypervisor, c) Network switch, d) User interface
15	II	Cloud trust models are most concerned with:	a) Data privacy, b) CPU usage, c) Visual appeal, d) Download speed
Unit III – Cloud Virtualization Technologies			
Sl. No	**Unit**	**Question**	**Options**
1	III	What is "hypervisor" in the context of virtualization?	a) App framework, b) Hardware to run VMs, c) Software that manages virtual machines, d) Data backup tool
2	III	Which is NOT a type of virtualization?	a) Hardware, b) Software, c) Network, d) Spooling
3	III	Which virtualization type allows multiple OS on the same hardware?	a) Desktop, b) Server, c) Storage, d) File
4	III	The primary isolation mechanism in virtualization is:	a) Ports, b) VMs, c) Encryption, d) Switches
5	III	In "Type-1" virtualization, the hypervisor runs:	a) On host OS, b) Directly on hardware, c) As browser extension, d) Only on cloud
6	III	Which is a benefit of server virtualization?	a) Increased hardware costs, b) Smoother patching/upgrades, c) Always slower performance, d) No management
7	III	What role does a VM snapshot serve?	a) Hardware upgrade, b) Quick system restore, c) Permanent backup, d) Increase disk space
8	III	Open-source hypervisor example is:	a) VMware, b) KVM, c) Hyper-V, d) Citrix
9	III	Which software provides automated deployment and management of VMs?	a) Apache, b) vSphere, c) Email client, d) Notepad

10	III	A benefit of storage virtualization is:	a) Limited file access, b) Flexible provisioning, c) Longer downtime, d) Higher hardware costs
11	III	In virtualization, "resource pooling" means:	a) Combine CPU/memory/storage for use by VMs, b) Local-only network, c) Single OS instance, d) No sharing
12	III	What is NOT true for container virtualization?	a) Lightweight, b) Shares OS kernel, c) Full machine simulation, d) Fast start-up
13	III	VM migration benefits include:	a) Improved cost and disaster recovery, b) Less uptime, c) Manual server work, d) OS compatibility lost
14	III	Implementation level virtualization refers to:	a) Hypervisor location, b) Data size, c) Regional datacenter, d) Programming language
15	III	"Virtual infrastructure requirements" mainly involve:	a) Network/storage/redundancy, b) Keyboard/mouse, c) GUI themes, d) None
Unit IV – IoT and Cloud Computing			
Sl. No	**Unit**	**Question**	**Options**
1	IV	What does IoT stand for?	a) Internet of Tools, b) Inter-Operator Technology, c) Internet of Things, d) Integrated Online Test
2	IV	Edge computing refers to:	a) Centralized processing, b) Processing close to data source/device, c) Offline backups, d) Mainframe tasks
3	IV	Fog computing is best described as:	a) Type of public cloud, b) Intermediate layer between edge devices and cloud, c) Browser plugin, d) Network cable
4	IV	What is the primary benefit of connecting IoT devices to the cloud?	a) Increased power use, b) Real-time access to data/services, c) Security decrease, d) None
5	IV	A cloud-enabled sensor in an IoT system is responsible for:	a) Running user apps, b) Gathering and sending data, c) Drawing UI, d) Rendering graphics
6	IV	The “edge architecture model” is most helpful for:	a) Device independence, b) Low-latency decisions without round-trip to cloud, c) Disk backup, d) Only for WiFi

7	IV	Which protocol is common for IoT cloud data transfer?	a) SMTP, b) MQTT, c) SHA, d) BIOS
8	IV	Fog computing enables:	a) Only reality checks, b) Pre-processing data before cloud upload, c) UI improvements, d) Less network use
9	IV	What distinguishes IoT from traditional networked devices?	a) Only wired connectivity, b) Autonomy and real-time response, c) Run only user programs, d) Proprietary clouds
10	IV	When "living on the edge" in IoT/cloud, the phrase means:	a) Using legacy devices, b) Processing near the source, c) Always on WiFi, d) No synching
11	IV	Devices at the edge commonly connect to:	a) Only LAN, b) Both edge and central cloud, c) Virtual kernel, d) Local storage
12	IV	A gateway device's main role in IoT–Cloud integration is:	a) App updates, b) Protocol translation and data transfer, c) User authentication, d) File backup
13	IV	Fog computing is considered an evolution of:	a) Mainframe, b) Data mining, c) Cloud computing, d) AR
14	IV	Which factor most limits latency in IoT systems?	a) Data center proximity, b) CPU brand, c) Screen size, d) App memory
15	IV	IoT device scalability is best achieved by:	a) Rigid architectures, b) Modular cloud solutions, c) Removing virtualization, d) Dedicated LAN
Unit V – Cloud Security			
Sl. No	**Unit**	**Question**	**Options**
1	V	Which is a major security risk unique to cloud computing?	a) Multi-tenancy resource sharing, b) Only local attacks, c) Single user per server, d) Zero backup issues
2	V	SaaS security threats are often related to:	a) Device drivers, b) Application-level vulnerabilities, c) Hardware ports, d) Only bandwidth
3	V	Security "monitoring" in the cloud involves:	a) Only checking uptime, b) Tracking activities and alerting on anomalies, c) Changing color schemes, d) UI updates
4	V	Identity management in cloud security mostly refers to:	a) Assigning usernames only, b) Granting proper access and authentication, c) VM deployment, d) IP filtering

5	V	What is a "risk assessment" in the context of cloud security?	a) Estimating insurance cost, b) Identifying and evaluating potential threats, c) Measuring temperature, d) Tracking user interface
6	V	Which standard is often used for cloud data encryption?	a) SSL/TLS, b) HTTP, c) FTP, d) ASCII
7	V	"Virtual machine escape" refers to:	a) Extraction of data from cloud, b) Exploit that allows breaking VM containment, c) Installing new OS, d) Backing up VM
8	V	Main cloud security architecture goal is:	a) Just network speed, b) Protect confidentiality, integrity, and availability, c) Increase costs, d) Lower storage
9	V	Which method is NOT a form of access control?	a) Role-based, b) Mandatory, c) Discretionary, d) Packet sniffing
10	V	Best method for secure application update delivery in cloud is:	a) USB drive, b) Digital signatures and secure channels, c) Email link sharing, d) Printed code
11	V	Which aspect is crucial for VM security in cloud?	a) Frequent OS updates, b) Ignoring patches, c) Removing logs, d) Only one user
12	V	Security in a multi-cloud environment is most complex because:	a) Same policies everywhere, b) Different providers and interfaces, c) Only private clouds used, d) Total isolation
13	V	Which is recommended for cloud data security?	a) Always use plaintext, b) Encrypt sensitive data at rest and in transit, c) Store only on desktop, d) Use only default passwords
14	V	"Security architecture design" in cloud should prioritize:	a) Access controls, b) Custom fonts, c) Fewer users, d) More local servers
15	V	Application security in the cloud mainly protects:	a) Just the user interface, b) The entire code and data workflow, c) Hardware only, d) System boot sequence

2 Marks

Unit I – Cloud Computing: Introduction

Sl. No	Unit	Question
1	I	Explain the difference between on-demand self-service and resource pooling in cloud computing with suitable examples.
2	I	List and briefly explain any two essential characteristics that make cloud computing unique from traditional computing.
3	I	How does service oriented architecture (SOA) support scalability in cloud environments?
4	I	Outline the main challenges organizations face during initial cloud migration.
5	I	Explain how the elasticity of cloud computing benefits seasonal businesses.
6	I	What role does virtualization play in enabling cloud computing?
7	I	Compare the security risks of public cloud and private cloud models.
8	I	Describe the role of APIs in cloud service delivery.
9	I	How does the pay-as-you-go model influence IT budgeting in cloud environments?
10	I	Identify two limitations of cloud computing for real-time applications.
11	I	Explain any two stages in planning for cloud migration.
12	I	Why is multi-tenancy both a strength and a challenge for cloud providers?
13	I	Describe briefly how disaster recovery is enhanced by cloud solutions.
14	I	How can monitoring tools help improve cloud service reliability?

15	I	State two reasons why cloud computing is vital for startup companies.

Unit II – Deployment & Service Models

Sl. No	Unit	Question
1	II	Distinguish between IaaS, PaaS, and SaaS with relevant examples.
2	II	Explain the importance of SLAs (Service Level Agreements) in cloud service models.
3	II	Compare data isolation techniques in public and hybrid cloud deployments.
4	II	Describe how a community cloud supports organizations with similar requirements.
5	II	What challenges may arise when integrating legacy systems with cloud platforms?
6	II	List two advantages and one disadvantage of using PaaS for web app development.
7	II	How does cloud bursting improve efficiency for enterprise workloads?
8	II	Explain the role of hypervisors in IaaS cloud model deployment.
9	II	What considerations must be made for regulatory compliance in cloud data storage?
10	II	Illustrate with a scenario when hybrid cloud would be the preferred solution.
11	II	Describe steps to secure SaaS applications from unauthorized access.
12	II	Why is vendor lock-in a concern for organizations using cloud services?
13	II	State two factors that influence service model selection for a new business.
14	II	How can monitoring and automation enhance cloud resource management?

15	II	Give examples of two security responsibilities faced by users in public cloud.

Unit III – Virtualization Technology

Sl. No	Unit	Question
1	III	Explain the difference between Type-1 and Type-2 hypervisors with examples.
2	III	How does VM live migration benefit cloud operations?
3	III	Outline any two disadvantages of server virtualization.
4	III	Describe the steps to create and restore a VM snapshot.
5	III	Why is resource pooling essential in virtualization?
6	III	How do containers differ from traditional virtual machines in terms of resource use?
7	III	State two factors influencing hypervisor performance.
8	III	Explain with a scenario how storage virtualization improves disaster recovery.
9	III	What is the significance of network virtualization in cloud computing?
10	III	List and describe two open-source virtualization platforms.
11	III	How do resource allocation policies affect VM deployment efficiency?
12	III	Illustrate with a use case when container technology is preferable in cloud deployments.
13	III	What is meant by 'virtual appliance' and its role in cloud infrastructure?
14	III	Explain how virtualization contributes to energy efficiency in a datacenter.
15	III	Identify two main challenges in managing large-scale virtualized environments.

Unit IV – IoT and Cloud Computing

Sl. No	Unit	Question

1	IV	Explain how edge computing reduces latency for IoT applications.
2	IV	Describe the main benefits of integrating IoT with cloud computing platforms.
3	IV	State two challenges in securing IoT devices connected to cloud services.
4	IV	How does fog computing address limitations in cloud-only IoT architectures?
5	IV	Provide an example where real-time analytics is vital in an IoT cloud deployment.
6	IV	Why is scalability a critical concern in IoT–cloud systems?
7	IV	Outline two protocols used for cloud-based IoT data communication.
8	IV	Explain the role of IoT gateways in integrating edge devices and cloud.
9	IV	Discuss two factors that affect connectivity reliability in IoT–cloud systems.
10	IV	How does cloud-enabled remote monitoring improve industrial IoT deployments?
11	IV	Identify two privacy issues arising in large-scale cloud–IoT deployments.
12	IV	Explain how device identity management supports security in cloud IoT.
13	IV	State two considerations for device firmware updates over cloud.
14	IV	Describe the typical data flow from IoT sensor to cloud analytics platform.
15	IV	What is the significance of data aggregation in scalable cloud IoT systems?

Unit V – Cloud Security

Sl. No	Unit	Question

1	V	Distinguish between data confidentiality and data integrity in cloud security.
2	V	List and explain two common cloud security threats organizations face today.
3	V	How does encryption at rest protect cloud-stored data from unauthorized access?
4	V	Describe measures to mitigate insider threats in cloud environments.
5	V	State two best practices for secure cloud API development.
6	V	Why is multi-factor authentication important in cloud services?
7	V	Outline ways to ensure compliance with data protection laws in cloud deployments.
8	V	How can organizations detect and respond to cloud-based denial-of-service attacks?
9	V	Explain the concept of 'shared responsibility' in cloud security models.
10	V	Discuss two challenges of securing data in multi-cloud environments.
11	V	Describe the security risks associated with virtual machine escape attacks.
12	V	State two methods to audit and monitor cloud access logs effectively.
13	V	How do cloud providers enforce isolation between tenant workloads?
14	V	Explain with examples how regulatory compliance affects cloud storage architecture.
15	V	What is the role of regular patch management for cloud infrastructure security?

4 Marks

Unit I – Cloud Computing: Introduction		
Sl. No	**Unit**	**Question**
1	I	Compare 'cloud elasticity' with 'cloud scalability', and explain with real-world examples how each affects organizational growth.
2	I	Discuss the impact of choosing a poor cloud service provider and describe essential criteria for evaluating providers.
3	I	Propose a stepwise migration plan for a legacy on-premises system to a cloud-native architecture, identifying key challenges.
4	I	Explain the role of APIs and SDKs in custom cloud application development and integration for modern enterprises.
5	I	Illustrate how disaster recovery is executed in cloud platforms, focusing on both backup strategies and failover mechanisms.
6	I	How can organizations use cloud monitoring tools to improve service reliability and security? Provide two concrete use cases.
7	I	Evaluate the environmental sustainability benefits and challenges of large-scale cloud infrastructure adoption.
8	I	Assess the risks and benefits of implementing multi-cloud strategies for business continuity.
9	I	Enumerate main compliance regulations that affect cloud computing and explain why ongoing compliance assessment is essential.
10	I	How can Zero Trust security models enhance cloud infrastructure security? Illustrate with implementation steps.

Unit II – Deployment & Service Models

Sl. No	Unit	Question
1	II	Design a decision matrix for selecting between IaaS, PaaS, and SaaS for a startup, including criteria such as scalability, security, and control.
2	II	Critically discuss vendor lock-in in cloud platforms and suggest practical strategies for mitigation.
3	II	Explain with examples how cloud bursting can be orchestrated for handling unexpected peak loads.
4	II	Analyze the role of automated scripting and orchestration tools in managing cloud deployments at scale.
5	II	Compare data security challenges unique to hybrid and multi-cloud architectures, and provide recommendations.
6	II	Propose a cloud deployment solution for a multinational company with strict compliance needs.
7	II	Evaluate the effectiveness of SLAs and performance monitoring in ensuring service reliability for mission-critical cloud applications.
8	II	Discuss the practical importance of regular cloud configuration reviews and automation in preventing misconfigurations.
9	II	Outline methods for securely integrating legacy systems with cloud environments and minimizing security risks.
10	II	How can role-based access control (RBAC) and least privilege principles strengthen cloud service management?

Unit III – Virtualization Technology

Sl. No	Unit	Question
1	III	Compare containerization and VM virtualization in terms of resource efficiency, portability, and security.

2	III	Design a scalable virtualized environment for a cloud-based web app: show components, explain management workflows.
3	III	How can live migration of VMs be securely managed to minimize downtime and protect data?
4	III	Discuss the impact of network virtualization on resource pooling and service isolation in cloud datacenters.
5	III	Evaluate scenarios where serverless computing might supersede traditional virtualization approaches for businesses.
6	III	Propose an energy-efficient virtualization solution for a small business seeking cost-effective, scalable infrastructure.
7	III	Analyze how micro-segmentation within virtualized networks enhances cloud security.
8	III	Outline the challenges of integrating container orchestration (e.g., Kubernetes) with legacy VM infrastructures.
9	III	How does snapshotting and backup management for VMs and containers ensure business continuity?
10	III	Assess factors influencing hypervisor selection for high-performance cloud-hosted environments.

Unit IV – IoT and Cloud Computing

Sl. No	Unit	Question
1	IV	Examine the architecture of a typical cloud-enabled IoT system, highlighting data flows and security checkpoints.
2	IV	How does fog computing complement edge and cloud computing for scalable IoT deployments? Provide a comparative assessment.

3	IV	Propose a monitoring solution using cloud analytics for real-time IoT device performance and anomaly detection.
4	IV	Discuss two key challenges in cloud-based IoT firmware management and propose strategies to address them.
5	IV	How can AI-driven cloud analytics improve predictive maintenance for industrial IoT applications?
6	IV	Explain the privacy and security challenges unique to large-scale IoT deployments in public clouds.
7	IV	Compare protocol choices for cloud–IoT communication (MQTT, HTTP, CoAP) and their fit for different use cases.
8	IV	Design a simple cloud-based workflow for remote configuration and update of IoT devices.
9	IV	Analyze two energy management strategies in IoT–cloud integration to minimize cost and overhead.
10	IV	What are the implications of data residency laws for global IoT cloud deployments?

Unit V – Cloud Security

Sl. No	Unit	Question
1	V	Assess how implementing the Zero Trust approach reduces risk in cloud security. Include steps for implementation.
2	V	Illustrate the process of enforcing encryption for both data at rest and in transit in cloud platforms.
3	V	Compare best-practice identity management strategies for multi-cloud versus single-cloud environments.
4	V	Outline the steps and considerations for conducting regular cloud penetration testing within an organization.

5	V	Discuss the challenges of compliance and audit in cloud security for global organizations and propose solutions.
6	V	Create a cloud incident response plan featuring monitoring, containment, and recovery phases for a SaaS platform.
7	V	How can continuous monitoring and log management techniques strengthen cloud infrastructure defenses?
8	V	Analyze the role of role-based access and least privilege principles in preventing cloud data breaches.
9	V	Critically evaluate two emerging threats in cloud security and outline mitigation approaches.
10	V	What are the main regulatory frameworks affecting cloud security, and how does regular compliance assessment benefit organizations?

10 Marks

Unit I – Cloud Computing: Introduction

Sl. No	Unit	Question
1	I	Your university wants to host its learning management platform for fluctuating student usage, ensuring secure, highly available access while minimizing costs. Propose a complete cloud solution, describe the deployment model, scalability features, and security controls, and support your answer with a block diagram.
2	I	A startup is moving its employee productivity suite from desktops to the cloud. Design a migration and adoption plan that covers risk assessment, training, backup, and support strategies, including diagrams or workflows to justify your approach.

Unit II – Deployment & Service Models

Sl. No	Unit	Question
1	II	An organization operates globally and needs to deploy a business process app that serves users in different legal jurisdictions. Design a multi-region cloud deployment (including the selection of service and deployment models) to ensure compliance, data locality, and performance. Illustrate with a suitable architecture diagram.
2	II	Your company is facing high cloud service costs due to inefficient use of IaaS resources. Develop and explain a stepwise strategy to optimize resource usage and costs without sacrificing critical application performance or availability.

Unit III – Virtualization Technology

Sl. No	Unit	Question

1	III	A client wants to improve disaster recovery and reduce downtime for its on-premises datacenter with virtualization. Propose and diagram a solution using cloud-integrated virtualized backups, VM clustering, and automated failover. Explain your design and why you selected each component.
2	III	Design a virtualized multi-tenant environment for a cloud provider that must meet strict isolation, resource flexibility, and performance guarantees for its customers. Justify the choices of virtualization type(s), network configuration, and monitoring needed.

Unit IV – IoT and Cloud Computing

Sl. No	Unit	Question
1	IV	You are tasked with architecting a city-wide smart traffic system leveraging IoT sensors and cloud analytics. Develop a high-level architecture showing data flow from device to cloud, real-time processing elements, and security features. Justify your design and provide a detailed diagram.
2	IV	A manufacturing firm needs scalable, secure, real-time monitoring of hundreds of machines using IoT and cloud integration. Propose a solution including network design, cloud services used, and edge computing considerations, and justify how your approach addresses latency, scalability, and data privacy.

Unit V – Cloud Security

Sl. No	Unit	Question

1	V	Your company stores and processes sensitive customer data in the cloud. Draft a comprehensive security architecture plan that covers data encryption, access management, monitoring, and incident response. Include a diagram and explain how each measure mitigates specific risks.
2	V	Imagine your organization must comply with multiple international regulations (like GDPR/PCI DSS) when using cloud services. Devise a stepwise compliance strategy, indicating how cloud features and third-party tools support legal and auditing requirements.