

SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)
SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF INFORMATION TECHNOLOGY

(Common to CSE)

QUESTION BANK



VII SEMESTER

PIT205- SECURITY AND PRIVACY IN CLOUD

Regulation – 2023

Academic Year 2026– 2027 (odd Semester)

Prepared by

Mr.S.Suresh Kumar, Asst.Prof(Sr.G)/IT

Mrs.R.Vijayalakshmi, Asst.Prof(O.G)/CSE



SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

DEPARTMENT OF INFORMATION TECHNOLOGY



QUESTION BANK

SUBJECT CODE & NAME: PIT205- SECURITY AND PRIVACY IN CLOUD

SEM / YEAR: VII / IV

UNIT-I: FUNDAMENTALS OF CLOUD SECURITY CONCEPTS			
Overview of cloud security- Security Services - Confidentiality, Integrity, Authentication, Non- repudiation, Access Control - Basic of cryptography - Conventional and public-key cryptography, hash functions, authentication, and digital signatures.			
PART - A			
Q.no	Questions	BTL	Competence
1	Define cloud security.	BTL-1	Remembering
2	What is confidentiality in cloud security?	BTL-1	Remembering
3	Mention any two goals of cryptography.	BTL-1	Remembering
4	What is access control in the context of cloud computing?	BTL-1	Remembering
5	Differentiate between conventional and public-key cryptography.	BTL-2	Understanding
6	Define a hash function.	BTL-1	Remembering
7	What is the role of authentication in cloud security?	BTL-1	Remembering
8	What is non-repudiation?	BTL-1	Remembering
9	Define digital signature.	BTL-1	Remembering
10	State any two differences between symmetric and asymmetric encryption.	BTL-1	Remembering
11	Mention any four characteristics of secure cloud services.	BTL-1	Remembering
12	What is integrity in the context of cloud security?	BTL-1	Remembering
13	Mention any two threats to cloud security.	BTL-1	Remembering
14	What are the five security services provided by cloud computing?	BTL-1	Remembering
15	What are the two main types of cryptography?	BTL-1	Remembering
16	What are hash functions and how are they used in cloud security?	BTL-1	Remembering
17	Compare cloud security vs traditional network security	BTL-2	Understanding
18	Define Cryptography.	BTL-1	Remembering
19	List the applications of cryptography	BTL-1	Remembering

PART-B

Q.No	Questions	BTL	Competence
1	(i)Describe in detail the basic concepts of cryptography. (8) (ii) Explain the difference between conventional and public-key cryptography with suitable examples. (8)	BTL-4	Analyzing
2	Analyze the security services provided in cloud computing – confidentiality, integrity, authentication, non-repudiation, and access control.	BTL-4	Analyzing

3	Discuss hash functions and their importance in cloud security. How are they used in authentication and digital signatures?	BTL3	Applying
4	What is cloud security? Explain the various security mechanisms used to ensure safe data storage and transmission in the cloud.	BTL-4	Analyzing
5	Elaborate on the importance of digital signatures in cloud environments. How do they ensure authentication and integrity?	BTL3	Applying
6	Compare and contrast symmetric and asymmetric cryptography.	BTL-4	Analyzing
7	Discuss how public-key infrastructure (PKI) is used for secure communication in cloud environments.	BTL3	Applying
8	What is cryptography? Explain various cryptographic techniques used to enhance cloud security	BTL-4	Analyzing
9	Discuss various cloud security services with suitable examples.	BTL-4	Analyzing
10	Explain public-key cryptography with RSA algorithm.	BTL-4	Analyzing
11	Describe various hash functions and their applications.	BTL3	Applying
12	Compare digital signatures and message authentication codes.	BTL3	Applying
13	Explain different authentication mechanisms used in cloud computing.	BTL-4	Analyzing
14	Discuss the applications of cryptographic techniques in cloud security.	BTL-4	Analyzing
15	Discuss cloud security challenges and possible solutions.	BTL-4	Analyzing
16	Explain message authentication techniques.	BTL-4	Analyzing
17	Explain the working of symmetric key encryption with examples.	BTL-4	Analyzing

UNIT-II: SECURITY DESIGN AND ARCHITECTURE FOR CLOUD

Security design principles for Cloud Computing - Comprehensive data protection - End-to-end access control - Common attack vectors and threats - Network and Storage - Secure Isolation Strategies - Virtualization strategies - Inter-tenant network segmentation strategies - Data Protection strategies: Data retention, deletion and archiving procedures for tenant data, Encryption, Data Redaction, Tokenization, Obfuscation, PKI and Key.

PART – A

Q.No	Questions	BTL	Competence
1	Define Security Design Principles.	BTL-1	Remembering
2	What is comprehensive data protection?	BTL-1	Remembering
3	Define end-to-end access control.	BTL-1	Remembering
4	List common cloud attack vectors.	BTL-2	Understanding
5	What is secure isolation?	BTL-1	Remembering
6	Define virtualization security.	BTL-1	Remembering
7	What is tenant isolation?	BTL-1	Remembering
8	Define inter-tenant network segmentation.	BTL-1	Remembering
9	What is data retention?	BTL-1	Remembering
10	Define data deletion.	BTL-1	Remembering
11	What is data archiving?	BTL-1	Remembering
12	What is data encryption?	BTL-1	Remembering
13	Define data redaction.	BTL-1	Remembering
14	What is tokenization?	BTL-1	Remembering
15	Define obfuscation.	BTL-1	Remembering
16	What is PKI?	BTL-1	Remembering

17	What is key management?	BTL-1	Remembering
18	Mention any two virtualization threats.	BTL-2	Understanding
19	Differentiate tokenization and encryption.	BTL-2	Understanding
20	Differentiate redaction and obfuscation.	BTL-2	Understanding
21	List data protection strategies.	BTL-1	Remembering
22	State any four security design principles.	BTL-1	Remembering
23	What is storage security?	BTL-1	Remembering
24	Define network security.	BTL-1	Remembering

PART-B

Q.No		BTL	Competence
1	Explain security design principles for cloud computing.	BTL-4	Analyzing
2	Describe comprehensive data protection techniques.	BTL3	Applying
3	Explain end-to-end access control in cloud computing.	BTL-4	Analyzing
4	Discuss common attack vectors and threats in cloud computing.	BTL-4	Analyzing
5	Explain network security strategies in cloud computing.	BTL-4	Analyzing
6	Discuss storage security techniques.	BTL-4	Analyzing
7	Explain secure isolation strategies in cloud environments.	BTL-4	Analyzing
8	Describe virtualization security strategies.	BTL3	Applying
9	Explain inter-tenant network segmentation strategies.	BTL-4	Analyzing
10	Discuss data retention, deletion and archiving procedures.	BTL-4	Analyzing
11	Explain encryption techniques used in cloud security.	BTL-4	Analyzing
12	Describe tokenization, redaction and obfuscation techniques.	BTL3	Applying
13	Explain PKI architecture and applications in cloud security.	BTL-4	Analyzing
14	Discuss key management techniques.	BTL-4	Analyzing
15	Compare encryption and tokenization.	BTL3	Applying
16	Explain data protection life cycle in cloud computing.	BTL-4	Analyzing
17	Design a secure cloud architecture incorporating all security mechanisms.	BTL-6	Creating

UNIT-III: ACCESS CONTROL AND IDENTITY MANAGEMENT

Access control requirements for Cloud infrastructure - User Identification - Authentication and Authorization - Roles-based Access Control - Multi-factor authentication - Single Sign-on, Identity Federation - Identity providers and service consumers - Storage and network access control options - OS Hardening and minimization - Verified and measured boot - Intruder Detection and prevention.

PART – A

Q.No	Questions	BTL	Competence
1	Define Access Control.	BTL-1	Remembering
2	What is Identity Management?	BTL-1	Remembering
3	Define User Identification.	BTL-1	Remembering
4	What is Authentication?	BTL-1	Remembering
5	Define Authorization.	BTL-1	Remembering
6	What is Role-Based Access Control (RBAC)?	BTL-1	Remembering
7	Define Multi-Factor Authentication.	BTL-1	Remembering
8	What is Single Sign-On (SSO)?	BTL-1	Remembering
9	Define Identity Federation.	BTL-1	Remembering
10	What is an Identity Provider?	BTL-1	Remembering
11	Define Service Provider.	BTL-1	Remembering
12	What is storage access control?	BTL-1	Remembering
13	What is network access control?	BTL-1	Remembering
14	Define OS Hardening.	BTL-1	Remembering
15	What is OS minimization?	BTL-1	Remembering
16	Define Verified Boot.	BTL-1	Remembering
17	What is Measured Boot?	BTL-1	Remembering
18	Define Intrusion Detection System.	BTL-1	Remembering
19	What is Intrusion Prevention System?	BTL-1	Remembering
20	Differentiate IDS and IPS.	BTL-2	Understanding
21	Differentiate Authentication and Authorization.	BTL-2	Understanding
22	State advantages of RBAC.	BTL-1	Remembering
23	List any four identity management components.	BTL-2	Understanding
24	Mention benefits of MFA.	BTL-2	Understanding

PART-B

Q.No	Questions	BTL	Competence
1	Explain cloud access control requirements.	BTL-4	Analyzing
2	Discuss authentication and authorization techniques.	BTL-4	Analyzing
3	Explain RBAC architecture with examples.	BTL-4	Analyzing
4	Explain Multi-Factor Authentication.	BTL-4	Analyzing
5	Discuss Single Sign-On architecture.	BTL-4	Analyzing
6	Explain Identity Federation in cloud computing.	BTL-4	Analyzing
7	Discuss Identity Providers and Service Providers.	BTL-4	Analyzing
8	Explain storage and network access control mechanisms.	BTL-4	Analyzing
9	Describe OS hardening techniques.	BTL3	Applying
10	Explain verified and measured boot process.	BTL-4	Analyzing
11	Explain Intrusion Detection Systems.	BTL-4	Analyzing
12	Explain Intrusion Prevention Systems.	BTL-4	Analyzing
13	Compare IDS and IPS.	BTL3	Applying
14	Explain identity management architecture.	BTL-4	Analyzing
15	Discuss cloud identity lifecycle management.	BTL-4	Analyzing
16	Explain modern authentication techniques used in cloud computing.	BTL-4	Analyzing
17	Design a secure identity and access management framework.	BTL-6	Creating

UNIT-IV: CLOUD SECURITY DESIGN PATTERNS			
Introduction to Design Patterns, Cloud bursting, Geo-tagging, Secure Cloud Interfaces, Cloud Resource Access Control, Secure On-Premise Internet Access, Secure External Cloud.			
PART - A			
Q.no	Questions	BTL	Competence
1	Define Design Pattern.	BTL-1	Remembering
2	What is Cloud Bursting?	BTL-1	Remembering
3	Define Geo-tagging.	BTL-1	Remembering
4	What is Secure Cloud Interface?	BTL-1	Remembering
5	Define Cloud Resource Access Control.	BTL-1	Remembering
6	What is Secure On-Premise Internet Access?	BTL-1	Remembering
7	Define Secure External Cloud.	BTL-1	Remembering
8	State the benefits of cloud bursting.	BTL-1	Remembering
9	Mention applications of geo-tagging.	BTL-2	Understanding
10	What are cloud APIs?	BTL-1	Remembering
11	Define API security.	BTL-1	Remembering
12	What is secure communication?	BTL-1	Remembering
13	List cloud security design patterns.	BTL-2	Understanding
14	Differentiate private and public cloud interfaces.	BTL-2	Understanding
15	Define secure gateway.	BTL-1	Remembering
16	What is cloud firewall?	BTL-1	Remembering
17	What is VPN?	BTL-1	Remembering
18	Define Zero Trust architecture.	BTL-1	Remembering
19	State the importance of secure cloud interfaces	BTL-1	Remembering
20	Mention cloud resource threats.	BTL-2	Understanding
21	What is hybrid cloud security?	BTL-1	Remembering
22	What is API authentication?	BTL-1	Remembering
23	List secure external cloud features.	BTL-2	Understanding
24	State advantages of cloud security design patterns.	BTL-1	Remembering
PART-B			
Q.no	Questions	BTL	Competence
1	Explain cloud security design patterns.	BTL-4	Analyzing
2	Explain cloud bursting architecture.	BTL-4	Analyzing
3	Discuss geo-tagging with applications.	BTL-4	Analyzing
4	Explain secure cloud interfaces.	BTL-4	Analyzing
5	Describe cloud resource access control mechanisms.	BTL-3	Applying
6	Explain secure on-premise Internet access.	BTL-4	Analyzing
7	Explain secure external cloud architecture.	BTL-4	Analyzing
8	Discuss API security techniques.	BTL-4	Analyzing
9	Explain hybrid cloud security design.	BTL-4	Analyzing
10	Discuss Zero Trust architecture in cloud computing.	BTL-4	Analyzing

11	Explain cloud gateway security.	BTL-5	Evaluating
12	Describe secure communication mechanisms.	BTL-5	Evaluating
13	Compare cloud bursting and hybrid cloud.	BTL-3	Applying
14	Explain VPN implementation in cloud security.	BTL-4	Analyzing
15	Design a secure cloud interface model.	BTL-6	Creating
16	Explain cloud access control design patterns.	BTL-4	Analyzing
17	Design a complete cloud security pattern architecture.	BTL-6	Creating

UNIT-V: MONITORING, AUDITING AND MANAGEMENT

UNIT-V: MONITORING, AUDITING AND MANAGEMENT 9 Proactive activity monitoring - Incident Response, Monitoring for unauthorized access, malicious SRM VEC: R2023 IT 196 traffic, abuse of system privileges - Events and alerts - Auditing – Record generation, Reporting and Management, Tamper-proofing audit logs, Quality of Services, Secure Management, User management, Identity management, Security Information and Event Management.

PART - A

Q.no	Questions	BTL	Competence
1	Define activity monitoring.	BTL-1	Remembering
2	What is Incident Response?	BTL-1	Remembering
3	Define unauthorized access.	BTL-1	Remembering
4	What is malicious traffic?	BTL-1	Remembering
5	Define privilege abuse.	BTL-1	Remembering
6	What is an event?	BTL-1	Remembering
7	Define alert.	BTL-1	Remembering
8	What is auditing?	BTL-1	Remembering
9	Define audit log.	BTL-1	Remembering
10	What is tamper-proof logging?	BTL-1	Remembering
11	Define record generation.	BTL-1	Remembering
12	What is reporting?	BTL-1	Remembering
13	Define Quality of Service (QoS).	BTL-1	Remembering
14	What is secure management?	BTL-1	Remembering
15	Define user management.	BTL-1	Remembering
16	What is identity management?	BTL-1	Remembering
17	Define SIEM.	BTL-1	Remembering
18	Mention SIEM components.	BTL-2	Understanding
19	Differentiate events and alerts.	BTL-2	Understanding
20	Differentiate monitoring and auditing.	BTL-2	Understanding
21	State advantages of SIEM.	BTL-1	Remembering
22	Mention the phases of incident response.	BTL-2	Understanding
23	List monitoring tools used in cloud security.	BTL-2	Understanding
24	State the importance of audit logs.	BTL-1	Remembering

PART-B

Q.no	Questions	BTL	Competence
1	Explain proactive activity monitoring in cloud security.	BTL-4	Analyzing
2	Explain the incident response life cycle.	BTL-4	Analyzing

3	Discuss monitoring techniques for unauthorized access.	BTL-4	Analyzing
4	Explain malicious traffic detection methods.	BTL-4	Analyzing
5	Discuss abuse of system privilege monitoring.	BTL-4	Analyzing
6	Explain event and alert management.	BTL-4	Analyzing
7	Discuss cloud auditing procedures.	BTL-4	Analyzing
8	Explain record generation and reporting mechanisms.	BTL-4	Analyzing
9	Describe tamper-proof audit logging.	BTL-3	Applying
10	Explain Quality of Service (QoS) in cloud security.	BTL-4	Analyzing
11	Discuss secure management techniques.	BTL-4	Analyzing
12	Explain user and identity management.	BTL-4	Analyzing
13	Explain the architecture and working of Security Information and Event Management (SIEM).	BTL-4	Analyzing
14	Compare monitoring and auditing.	BTL-3	Applying
15	Explain cloud security operations and management.	BTL-4	Analyzing
16	Design a secure monitoring and auditing framework for cloud environments.	BTL-6	Creating
17	Discuss best practices for cloud security monitoring, auditing, and incident management with suitable examples. (BTL5)	BTL-4	Analyzing