Printed Page:- **Subject Code:- ACSCY0602**

Roll. No:

NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA

(An Autonomous Institute Affiliated to AKTU, Lucknow)

B.Tech

SEM: VI - THEORY EXAMINATION (20.... - 20....)

Subject: Cloud Security and Privacy

Time: 3 Hours **Max. Marks: 100**

General Instructions:

IMP: *Verify that you have received the question paper with the correct course, code, branch etc.*

1. *This Question paper comprises of* ***three Sections -A, B, & C.*** *It consists of Multiple Choice Questions (MCQ's) & Subjective type questions.*

2. *Maximum marks for each question are indicated on right -hand side of each question.*

3. *Illustrate your answers with neat sketches wherever necessary.*

4. *Assume suitable data if necessary.*

5. *Preferably, write the answers in sequential order.*

6. *No sheet should be left blank. Any written material after a blank sheet will not be evaluated/checked.*

SECTION-A 20

1. Attempt all parts:-

1-a. Software as a Service (SaaS) provides (CO1, K1) 1

(a) Network hardware
(b) Online applications
(c) Data centers
(d) Firewalls

1-b. Data breaches in cloud environments often occur due to (CO1, K1) 1

(a) Weather
(b) Hardware quality
(c) Weak authentication
(d) Office size

1-c. Tool responsible for distributing containers across cloud instances is (CO2, K1) 1

(a) Virtual machine
(b) IAM
(c) Orchestrator
(d) SSH

1-d. IAM enforces access based on (CO2, K2) 1

(a) Username length
(b) Roles and permissions
(c) Email domains

(d) VPN

1-e. Suppression is typically used to achieve: (CO3, K2) 1

(a) k-anonymity
(b) Homogeneity
(c) Data expansion
(d) Tokenization

1-f. Perturbation is typically used to achieve: (CO3, K2) 1

(a) Data integrity
(b) Differential privacy
(c) Data normalization
(d) Data sorting

1-g. Biometric authentication uses: (CO4, K1) 1

(a) Username and password
(b) Fingerprint or face recognition
(c) IP address
(d) Network speed

1-h. OAuth 2.0 is used for: (CO4, K2) 1

(a) Network testing
(b) Email services
(c) Secure user authorization
(d) Phone calls

1-i. Define TLS in mobile communication. (CO5, K2) 1

(a) Transport Layer Security
(b) Total Layer Shield
(c) Transfer Line Safety
(d) Transport Logic Secure

1-j. Recognize an MDM feature. (CO5, K1) 1

(a) Video call
(b) Remote wipe
(c) Screenshot
(d) Music playback

2. Attempt all parts:-

2.a. Explain mobile computing? 2

2.b. List two security principles followed in cloud environments. 2

2.c. Discuss how perturbation techniques can contribute to achieving differential privacy. 2

2.d. Highlight the importance of runtime permission checks in Android. 2

.

2.e.	List two functions of mobile threat defense tools.	2
SECTION-B		30
3. Answer any five of the following:-		
3-a.	Describe network security in cloud environments. (CO1, K1)	6
3-b.	Describe the architecture of cloud computing in detail. (CO1, K2)	6
3-c.	Summarize the significance of endpoint security in cloud environments. (CO2, K2)	6
3-d.	Show how Cloud Access Security Brokers (CASB) enhance security and compliance. (CO2, K2)	6
3.e.	Analyze the limitations of Incognito when applied to datasets with high attribute dimensionality. (CO3, K3)	6
3.f.	Describe encryption techniques used for protecting mobile data at rest. (CO4, K3)	6
3.g.	Compare VPN and TLS in terms of mobile communication security. (CO5, K2)	6
SECTION-C		50
4. Answer any one of the following:-		
4-a.	Explain challenges of securing hybrid cloud environments. (CO1, K2)	10
4-b.	Explain in detail the lifecycle of cloud security policy development. (CO1, K2)	10
5. Answer any one of the following:-		
5-a.	Assess the role of mobile security frameworks in protecting cloud-based applications. (CO2, K3)	10
5-b.	Express insights into securing virtualization platforms and orchestration tools within cloud environments. (CO2, K2)	10
6. Answer any one of the following:-		
6-a.	Illustrate the trade-offs between utility and privacy in anonymization outputs produced by Incognito and Datafly. (CO3, K2)	10
6-b.	Present a comparative study on the performance of Mondrian and Greedy K-members when scaling to large enterprise datasets. (CO3, K3)	10
7. Answer any one of the following:-		
7-a.	Describe the implications of insecure authorization logic in mobile apps. (CO4, K2)	10
7-b.	Discuss the architectural components of Android and their role in maintaining system-level security. (CO4, K3)	10
8. Answer any one of the following:-		
8-a.	Illustrate how biometric data is stored and protected in mobile devices. (CO5, K3)	10
8-b.	Compare TLS and SSL in terms of mobile security and usability. (CO5, K2)	10