

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|

**NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA**

**(An Autonomous Institute Affiliated to AKTU, Lucknow)**

**B.Tech**

**SEM: VI - THEORY EXAMINATION (2022-2023 )**

**Subject: Privacy and Security in IoT**

**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. | What is a common security concern associated with IoT devices? (CO1)                                                                                                                                                                                                                                                             | 1 |
|      | <ul style="list-style-type: none"> <li>(a) Poor battery life</li> <li>(b) Insufficient processing power</li> <li>(c) Insecure communication channels</li> <li>(d) Limited memory capacity</li> </ul>                                                                                                                             |   |
| 1-b. | What is a fault tree? (CO1)                                                                                                                                                                                                                                                                                                      | 1 |
|      | <ul style="list-style-type: none"> <li>(a) A graphical representation of a system's failure modes</li> <li>(b) A list of all possible failure modes of a system</li> <li>(c) A diagram showing the sequence of events in a system failure</li> <li>(d) A diagram showing the likelihood of a system failure occurring</li> </ul> |   |
| 1-c. | Which of the following is an example of a data protection security control in an enterprise IoT cloud security architecture? (CO2)                                                                                                                                                                                               | 1 |
|      | <ul style="list-style-type: none"> <li>(a) Encryption of data at rest and in transit</li> <li>(b) Access control</li> </ul>                                                                                                                                                                                                      |   |

- (c) Network segmentation and isolation
- (d) Physical security controls
- 1-d. What is the primary purpose of an IoT cloud platform? (CO2) 1
  - (a) To provide storage and computing resources for IoT devices
  - (b) To enable real-time monitoring and control of IoT devices
  - (c) To facilitate the collection, storage, and analysis of data from IoT devices
  - (d) To provide a user interface for interacting with IoT devices
- 1-e. Which of the following is a disadvantage of asymmetric encryption? (CO3) 1
  - (a) It is slower than symmetric encryption
  - (b) It requires more processing power than symmetric encryption
  - (c) It requires secure key exchange
  - (d) It is vulnerable to brute force attacks
- 1-f. Which of the following is a key management function? (CO3) 1
  - (a) Key generation
  - (b) Key distribution
  - (c) Key revocation
  - (d) All of the above
- 1-g. Which of the following is a common technique for improving data aggregation in large-scale data dissemination? (CO4) 1
  - (a) MapReduce
  - (b) Data filtering
  - (c) Data normalization
  - (d) Data compression
- 1-h. What is the purpose of a peer-to-peer trust model? (CO4) 1
  - (a) To establish trust between two devices without the need for a central authority
  - (b) To create a secure connection between two devices
  - (c) To ensure that data transmitted between devices is encrypted
  - (d) To provide a certificate-based trust model for IoT devices
- 1-i. What does SNMP stand for? (CO5) 1
  - (a) Simple Network Monitoring Protocol
  - (b) Standard Network Management Protocol
  - (c) Simple Network Management Protocol

(d) Standard Network Monitoring Protocol

- 1-j. Which of the following is not a benefit of using a firewall? (CO5) 1
- (a) Increased network performance
  - (b) Protection against unauthorized access
  - (c) Protection against malware
  - (d) Increased network reliability

**2. Attempt all parts:-**

- 2.a. Explain "over-the-air" attacks. (CO1) 2
- 2.b. How firewalls protect against attacks? (CO2) 2
- 2.c. What is a digital signature? (CO3) 2
- 2.d. Enlist the role of encryption in node authentication. (CO4) 2
- 2.e. Describe different types of attacks against IoT systems. (CO5) 2

**SECTION B**

**30**

**3. Answer any five of the following:-**

- 3-a. Explain IoT security along with the privacy concerns in IoT applications. (CO1) 6
- 3-b. What are some common vulnerabilities in IoT systems? How it can be reduced? (CO1) 6
- 3-c. What are the challenges in IoT cloud security architecture? Explain in detail. (CO2) 6
- 3-d. How do cloud service provide security and what are the benefits of using cloud services? (CO2) 6
- 3.e. How do cryptographic primitives improve the security? (CO3) 6
- 3.f. How do lightweight cryptographic schemes ensure confidentiality? (CO4) 6
- 3.g. Explain SMI and MIB in detail. (CO5) 6

**SECTION C**

**50**

**4. Answer any one of the following:-**

- 4-a. What are some common threats to transport encryption, and how can these threats be mitigated? (CO1) 10
- 4-b. Describe the attack tree methodology, and explain how it can be used to analyze and prevent attacks on transport encryption systems. (CO1) 10

**5. Answer any one of the following:-**

- 5-a. What are the benefits of using cloud services for IoT implementation? Explain in detail. (CO2) 10

5-b. What is an enterprise IoT cloud security architecture? Explain with suitable diagram. (CO2) 10

**6. Answer any one of the following:-**

6-a. What is a certificate authority and how does it play a role in digital signatures? Explain in detail. (CO3) 10

6-b. What is the role of hashing in password storage and why is it important for security? explain with example. (CO3) 10

**7. Answer any one of the following:-**

7-a. How do privacy laws and regulations impact data dissemination, and what are the key considerations for organizations when sharing data? (CO4) 10

7-b. What role do standards and regulations play in establishing trust in IoT? Explain in detail. (CO4) 10

**8. Answer any one of the following:-**

8-a. What are the different types of cryptographic algorithms, and how do they differ? Explain in detail. (CO5) 10

8-b. What are the key components of a secure key distribution and certification system for IoT? Explain in detail (CO5) 10