PAPER ID-310047

Roll No: [ ][ ][ ][ ][ ][ ][ ][ ][ ][ ][ ][ ][ ]

BTECH
(SEM VII) THEORY EXAMINATION 2024-25
IOT SECURITY

TIME: 3 HRS   **M.MARKS: 100**

Note: Attempt all Sections. In case of any missing data; choose suitably.

SECTION A

1.   **Attempt *all* questions in brief.**   **2 x 10 = 20**

Q no.	Question	CO	Level
a.	How do primary security requirements in IoT architecture differ from traditional IT systems?	1	K_1, K_2
b.	Explain the significance of access control in IoT systems.	1	K_1, K_2
c.	What are the respective advantages and limitations of asymmetric encryption techniques for IoT application?	2	K_2
d.	Discuss the implications of hash functions in ensuring data integrity and authenticity in IoT systems.	2	K_2
e.	How does identity lifecycle in IoT systems differ from traditional IAM practices?	3	K_2
f.	How can secure storage and management of credentials be achieved?	3	K_2
g.	Analyze the role of regulatory frameworks in ensuring privacy in IoT applications.	4	K_3
h.	How can the challenges of implementing privacy-preserving mechanisms in resource-constrained IoT devices be addressed?	4	K_3
i.	Analyze the challenges of ensuring data confidentiality and integrity in cloud-enabled IoT systems.	5	K_3
j.	How effective are the security controls offered by major cloud service providers in addressing IoT-specific risks?	5	K_3

SECTION B

2.   **Attempt any *three* of the following:**   **10 x 3 = 20**

Q no.	Question	CO	Level
a.	Evaluate the role of transport encryption in safeguarding data integrity and confidentiality in IoT systems. How does it address IoT-specific vulnerabilities?	1	K_1, K_2
b.	Describe the integration of cryptographic controls into IoT communication protocols. How do these controls enhance security?	2	K_2
c.	Evaluate the significance of identity federation in IoT ecosystems. How does it enable interoperability across devices and platforms?	3	K_2
d.	Examine lightweight and robust privacy schemes for wearable body sensor networks. What specific challenges do these schemes address?	4	K_3
e.	Investigate the use of blockchain in enhancing security for cloud-based IoT ecosystems. What are the benefits and challenges of this approach?	5	K_3

SECTION C

3.   **Attempt any *one* part of the following:**   **10 x 1 = 10**

PAPER ID-310047

Roll No: | | | | | | | | | | | | |

BTECH
(SEM VII) THEORY EXAMINATION 2024-25
IOT SECURITY

TIME: 3 HRS   **M.MARKS: 100**

Q no.	Question	CO	Level
a.	Compare and contrast the nature of privacy concerns in IoT applications with those in traditional IT applications. Provide examples from healthcare and smart home domains.	1	K_1, K_2
b.	Explore the role of fault tolerance in IoT security. How do attack trees assist in designing fault-tolerant IoT systems?	1	K_1, K_2

4.   **Attempt any *one* part of the following:**   **10 x 1 = 10**

Q no.	Question	CO	Level
a.	Analyze how random number generation is critical for cryptographic operations in IoT. What methods ensure the generation of secure and unpredictable numbers?	2	K_2
b.	Discuss the process of key management in IoT systems. How does it ensure secure communication between resource-constrained nodes?	2	K_2

5.   **Attempt any *one* part of the following:**   **10 x 1 = 10**

Q no.	Question	CO	Level
a.	Compare role-based and attribute-based access control models for IoT applications. Which is more suitable for dynamic environments?	3	K_2
b.	Examine the interplay between IoT identity management and privacy. How can privacy-enhancing technologies support IAM in IoT?	3	K_2

6.   **Attempt any *one* part of the following:**   **10 x 1 = 10**

Q no.	Question	CO	Level
a.	Compare and contrast privacy preservation strategies for consumer IoT devices versus industrial IoT deployments.	4	K_3
b.	Discuss the importance of privacy-preserving data dissemination in IoT applications. What are the key challenges involved?	4	K_3

7.   **Attempt any *one* part of the following:**   **10 x 1 = 10**

Q no.	Question	CO	Level
a.	Evaluate the implications of multi-tenancy in cloud services on IoT security. How can isolation between tenants be ensured?	5	K_3
b.	Compare public, private, and hybrid cloud models for IoT deployments. What are the security considerations for each model?	5	K_3