PAPER ID-310324

Subject Code: BCIT056

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

BTECH
(SEM V) THEORY EXAMINATION 2024-25
PRIVACY AND SECURITY IN IOT

TIME: 3 HRS **M.MARKS: 70**

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

SECTION A

1. Attempt *all* questions in brief. 2 x 07 = 14

Q no.	Question	CO	Level
a.	Describe the specific attacks unique to IoT systems.	1	K_1, K_2
b.	How does transport encryption complement secrecy and secret-key capacity in secure communication?	1	K_1, K_2
c.	How does hashing ensure data integrity in resource-constrained environments?	2	K_1, K_2
d.	How do cryptographic primitives enable secure communication in IoT?	2	K_1, K_2
e.	Analyze the challenges of managing authentication credentials in IoT ecosystems.	3	K_1, K_2
f.	What are the key privacy concerns in IoT data dissemination?	4	K_1, K_2
g.	How can edge computing complement cloud security in IoT ecosystems?	4	K_1, K_2

SECTION B

2. Attempt any *three* of the following: 07 x 3 = 21

Q no.	Question	CO	Level
a.	What are the core security requirements for IoT architecture, and how do they differ across enabling technologies and IoT applications?	1	K_1, K_2
b.	Discuss the challenges of key management in IoT environments. How do lightweight key management solutions enhance system security?	2	K_1, K_2
c.	Describe the identity lifecycle in IoT systems. How does it ensure secure device onboarding and decommissioning?	3	K_1, K_2
d.	Discuss the trade-offs between privacy protection and system performance in IoT environments. Provide examples of robust privacy schemes.	4	K_1, K_2
e.	Discuss the implications of data sovereignty and compliance requirements in cloud-enabled IoT systems.	4	K_1, K_2

SECTION C

3. Attempt any *one* part of the following: 07 x 1 = 07

Q no.	Question	CO	Level
a.	What are the primary barriers to implementing robust access control in IoT, and how can emerging technologies address these challenges?	1	K_1, K_2

Roll No: □□□□□□□□□□□□□

BTECH
(SEM V) THEORY EXAMINATION 2024-25
PRIVACY AND SECURITY IN IOT

TIME: 3 HRS **M.MARKS: 70**

b.	Using attack and fault trees, evaluate a real-world IoT application to identify potential threats and propose mitigation strategies.	1	K_1, K_2

4. Attempt any *one* part of the following: 07 x 1 = 07

Q no.	Question	CO	Level
a.	Analyze the role of random number generation in IoT cryptography. How does it impact the overall security of cryptographic protocols?	2	K_1, K_2
b.	How do cryptographic techniques balance security and performance in IoT systems with constrained computational resources?	2	K_1, K_2

5. Attempt any *one* part of the following: 07 x 1 = 07

Q no.	Question	CO	Level
a.	How does the concept of least privilege apply to IoT access control? Provide examples of its implementation.	3	K_1, K_2
b.	Evaluate the effectiveness of different access control models in IoT systems. Which model is most suitable for a highly dynamic IoT environment?	3	K_1, K_2

6. Attempt any *one* part of the following: 07 x 1 = 07

Q no.	Question	CO	Level
a.	How do self-organizing IoT devices ensure security and trust without centralized control? Discuss potential vulnerabilities.	4	K_1, K_2
b.	Discuss the importance of transparency in IoT trust models. How does it influence user confidence and system adoption?	4	K_1, K_2

7. Attempt any *one* part of the following: 07 x 1 = 07

Q no.	Question	CO	Leve l
a.	How do cloud service offerings enhance IoT capabilities? Discuss the security implications of integrating IoT with cloud services.	4	K_1, K_2
b.	How do cloud service providers address the unique security needs of IoT applications? Provide examples of specific offerings.	4	K_1, K_2