Exam. Code: 1046
Sub. Code: 35462

2056

M.E. (Computer Science and Engineering - Cyber Security)

Second Semester

CSN-8206: Internet of Things Security

Time allowed: 3 Hours | Max. Marks: 50

NOTE: *Attempt five questions in all, including Question No. I which is compulsory and selecting two questions from each Section.*

Q1. a) Differentiate between cyber security and IoT security.
b) Draw and explain MQTT publish/subscribe model.
c) State and define the classic pillars of information assurance.
d) List three examples of functional security requirements to be added to product backlog.
e) Explain the role of cryptography in securing the IoT.
f) What are cipher suites?
g) State dynamic characteristics of an IoT environment.
h) State two attacks important to consider for threat profile: cloud system administrators and users.
i) List the potential front doors for data entry in AWS.
j) List 2 IoT-related protocols supported by Azure IoT Hub.

(10x1=10)

Section A:

Q2. a) Draw and explain in detail different IoT device lifecycle phases and relevant actors in each.
b) Draw the complete communication stack of IoT protocols. Explain it with a smart home example and describe the role of protocols at each layer involved in successful device-to-device communication.

(04+06)

Q3. a) Compare Fault tree and Attack tree.
b) State in detail the threat modelling process followed in an IoT system. Explain all the steps with reference to a smart parking system.

(03+07)

Q4. a) Draw the complete Secure IoT System Implementation Life Cycle.
b) Explain the roles of IoT Enterprise security administrator, device security administrator and network administrator.

(04+06)

Section B:

Q5. a) List the cryptographic primitives. Explain all with the help of diagrams and also name few solutions for each category.
b) Explain cryptographic key management using key handling topics, namely, key generation, key establishment, key derivation, key storage, key escrow, key lifetime and key zeroization.

(04+06)

Q6. a) Draw and explain the identity lifecycle for an IoT device.
b) What are public key infrastructures? How are they utilized in securing IAM deployments for the IoT?

(03+07)

Q7. Write a note on:
(a) AWS IoT
(b) Microsoft Azure IoT
(c) Cloud IoT Security Controls

(03+03+04)

x-x-x