VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

REG.NO.:

SLOT: A1 + TA1

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - I
FALL SEMESTER 2025-2026

Programme Name & Branch : B.Tech CSE and other specializations
Course Code and Course Name : BCSE314L - Privacy and Security in IoT
Faculty Name(s) : Prof. Swetha.N.G., Prof. Ganesh Shamrao Khekare
Class Number(s) : VL2025260102390, 2393
Date of Examination : 17.08.2025
Exam Duration : 90 minutes **Maximum Marks: 50**

General instruction(s):

- Answer All Questions
- M - Max mark; CO – Course Outcome; BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)
- Course Outcomes:
  CO1: Identify different Internet of Things technologies and their applications.
  CO2: Assess the need for Privacy and security model for the Internet of Things.

Q. No	Question	M	CO	BL
1.	Discuss the stages of the IoT Security Life Cycle with reference to a smart classroom environment. For each stage, provide a clear explanation along with relevant examples illustrating how security is managed for devices such as smart boards, surveillance cameras, biometric attendance systems, and teacher authentication modules.	10	CO 2	BL 1
2.	***Scenario 1:*** Unauthorized access to a smart door lock in a smart home environment ***Scenario 2:*** Unauthorized retrieval of confidential HR records from a corporate system For each scenario, construct a corresponding attack tree. Clearly define the root goal and decompose it into appropriate intermediate subgoals and basic attack actions, by following standard attack tree modelling conventions.	10	CO 1	BL 3
3.	In a smart city environment, seven environmental sensor nodes (M1 to M7) are deployed to monitor air quality across multiple zones. Nodes M4 and M6, situated in the central region, are designated as influential nodes with high trust values due to their strategic location and reliability. However, at a specific point in time, Node M4 and Node M7 are compromised, and begin disseminating falsified air quality data. Based on the above scenario, answer the following: a) Outline, in a step-by-step manner, how the Fusion-Based Defence Scheme detects the compromise of Nodes M4 and M7 through collective data analysis. b) Explain how the Sequential Defence Scheme identifies and confirms the presence of compromised nodes within the network. c) Between the two schemes, which do you consider more suitable for this scenario? Justify your answer.	10	CO 1	BL 3

VIT

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

REG.NO.:

SLOT: A1 + TA1

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - I
FALL SEMESTER 2025-2026

4.	In a VANET scenario, Roadside Units (RSUs) are deployed at 2 km intervals to monitor vehicular communication. A malicious vehicle attempts to spoof multiple identities in order to tamper with traffic analytics collected by the RSUs. Explain, in a structured step-by-step manner, how RSUs can utilize Received Signal Strength Indicator (RSSI) to detect such Sybil attacks. Support your explanation with a clear and labelled diagram illustrating the detection process.	10	CO 2	BL 4
5.	Consider a blockchain network consisting of 7 nodes (A,B,C,D,E,F,G) each node with a balance of 10 BTC. A transaction is initiated from Node A to Node B, involving a transfer of 7 BTC. The block is successfully mined by Node E using the Proof of Work (PoW) consensus mechanism and the reward for successful mining is 0.5 BTC (transaction fee paid by Node A). Based on the given scenario answer the following questions, a) Outline the complete process of block formation, starting from the broadcasting of the transaction to its successful addition to the blockchain. b) Explain the role of the previous block's hash in ensuring the integrity and validity of the new block. c) Find the updated BTC balances for Nodes A, B, and E after the block has been added to the chain.	10	CO 1	BL 3

****