VIT

Vellore Institute of Technology

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

REG.NO.:

SLOT: A2+TA2

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

CONTINUOUS ASSESSMENT TEST - 2

FALL SEMESTER 2025-2026

Programme Name & Branch	**: B.Tech CSE(IoT)**
Course Code and Course Name	**: BCSE 314L Privacy and Security in IoT**
Faculty Name(s)	**: Dr. Pushpa Gothwal and Dr. K. Ragavan**
Class Number(s)	**: VL2025260102391, VL2025260102394**
Date of Examination	**: 5.10.2025**
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 – Analyze, 5 – Evaluate, 6 – Create)
- Course Outcomes:
  CO2: Assess the need for Privacy and security model for the Internet of Things.
  CO4: Design security framework and solve IoT security issues

Q. No	Question	M	CO	BL
1.	A smart healthcare provider is considering adopting Blockchain applications to ensure secure storage of patient data and efficient access control for doctors and insurance companies. Illustrate a blockchain-based access control framework for this healthcare application. Highlight the key challenges in terms of scalability, privacy, and real-time access.	10	CO4	5
2.	A utility company deploys smart meters in residential homes to record electricity consumption every 15 minutes. While these meters help optimize energy distribution, they also raise privacy concerns: fine-grained consumption data can reveal occupant behaviors, appliance usage, or occupancy patterns.The utility wants to analyse aggregate energy usage without compromising individual household privacy. (i) Identify two major privacy threats associated with smart meter data. (ii) Describe three privacy-preserving approaches for smart meters. (iii) Discuss the trade-off between data utility and privacy for each approach. (iv) Propose a hybrid solution for the utility company that balances privacy preservation and energy usage analytics.	10	CO2	4
3.	A) In a smart city IoT deployment, 4 sensors (S1, S2, S3, S4) are reporting temperature data. The dataset is given as: • Sensor readings: S1 = 30°C, S2 = 32°C, S3 = 31°C, S4 = 29°C • Baseline values: S1 = 29°C, S2 = 32°C, S3 = 30°C, S4 = 30°C The sensor can only transmit if the reading is greater than 2 degrees Celsius. (i) Calculate the deviation of each sensor reading from its baseline. Determine which sensors will transmit data. (ii) Show the transmitted dataset after applying baseline dissemination (iii) Explain how this approach reduces communication overhead in IoT systems.Discuss how this technique contributes to privacy preservation in large-scale sensor networks. B) A smart building with 4 IoT sensors (P, Q, R, S) and the adjacency (communication) matrix: $M = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$	6+4	CO2	5

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

REG.NO.:

SLOT: A2+TA2

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - 2
FALL SEMESTER 2025-2026

	(i) Draw the spatial privacy graph for the network. (ii) If sensor R's data must be hidden from an adversary, apply a two-hop obfuscation strategy and show how privacy is preserved.			
4.	A)A healthcare startup is deploying a Mobile Wireless Body Sensor Network (MWBSN) to monitor patients' vital signs (e.g., heart rate, blood pressure, oxygen saturation). The data is collected via wearable sensors and transmitted to a central server for analysis. The network is part of a participatory sensing application, where multiple users' data are aggregated to detect health trends. Privacy is critical, as raw sensor data may reveal sensitive personal information. The startup plans to use lightweight and robust privacy schemes (i) Describe how the One-Time Permutation scheme preserves privacy while allowing aggregated analytics. (ii) Discuss the advantages and limitations of using lightweight schemes in MWBSN and participatory sensing applications. (B) A smart agriculture field is equipped with IoT sensors to monitor temperature, soil moisture, and humidity. The collected sensor data is transmitted to a cloud server for analysis. To protect sensitive information, the system applies a one-time permutation scheme on the dataset before transmission. Suppose the raw sensor readings for a given time slot are: {Temperature: 28,Moisture: 65, Humidity: 45} and a random permutation key P = {3, 1, 2} is used. (i) Find the permuted dataset that will be transmitted. (ii) Explain how the receiver can recover the original dataset using the permutation key. Briefly state how one-time permutation helps in ensuring privacy in IoT systems.	5+5	CO4	4
5.	A) Consider a dataset of 5 IoT sensor readings: {12, 20, 25, 30, 40,67,89,56,89,80}. Apply a one-time mask using a random key sequence {3, 7, 5, 2, 6,7,8,6,4,8}. Show the masked data and explain how the original readings can be recovered at the receiver side. Discuss how this scheme ensures privacy. B) An IoT temperature sensor uses an 8-bit one-time mask Due to an implementation flaw, the same mask was reused for two readings. Ciphertexts observed: C1=0x8D, C2=0xA6 C3=0xAB, C4=0x67, C5=0x89, C6=0x78, C7=0x30, C8=0x89 and the first plaintext value is 182. (i) Find the mask (ii) Recover the second plaintext P2, P3, P4, P5, P6, P7, P8 (iii) Briefly explain why mask reuse violates privacy in IoT.	5+5	CO4	5

****