REG.NO.:

VIT

Vellore Institute of Technology

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

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

CONTINUOUS ASSESSMENT TEST - II

FALL SEMESTER 2024-2025

SLOT: E1

Programme Name & Branch	: B.Tech - BBS
Course Code and Course Name	: CBS3002-Information Security
Faculty Name(s)	: Dr. K. Vimala Devi
Class Number(s)	: VL2024250103232
Date of Examination	: 17.10.2024
Exam Duration	: 90 minutes

Maximum Marks: 50

General instruction(s):

- Answer All Questions

Q. No	Question	M
1.	a) The credentials inputted are in an authentication system are either correct, or they're not. But what if the check fails entirely, say, because of an unexpected outage of electricity in the database server? Your code keeps running, but you get a "DB not found" error. Did you consider that? In the same scenario, what if, for example, your SQL query fails due to non-unicode characters that suddenly appeared as input? Explain how do you handle the above situations by following the appropriate design principle to make the system safe?	5
	b) The administrator of an eCommerce site, for example, should not be able to make purchases. And a user of the same site is promoted to the administrator role, to make purchases. He is altering the orders or give him selves, the free products. What design principle can be applied for the above scenario to make sure that the tasks are split into (and limited to) appropriate user types, though this principle could also apply to subsystems? Explain.	5
2.	Consider a client/server situation: the client sends a data request to the server; the server uses the data, performs some function, and sends the results (data) back to the client. Discuss about the confinement problem in the above situation. Write about the rule of transitive confinement and covert channel with example.	10

REG.NO.:

VIT

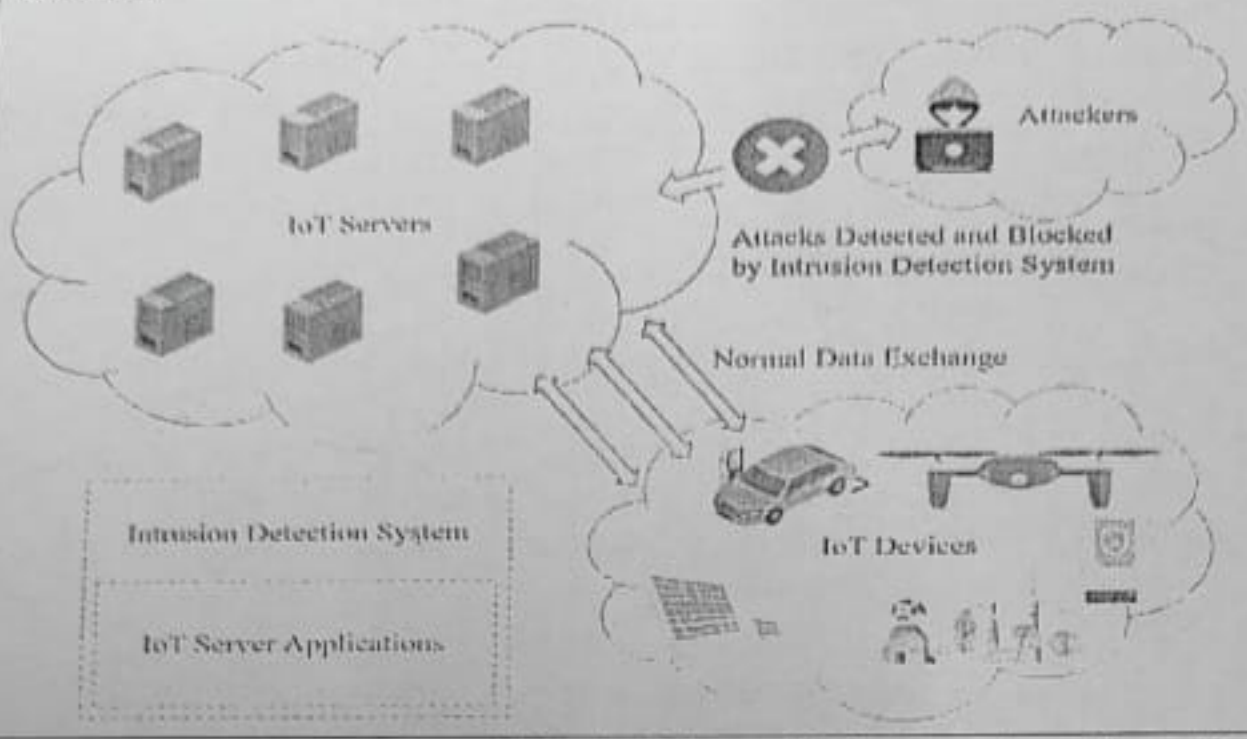
Vellore Institute of Technology

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

CONTINUOUS ASSESSMENT TEST - II

FALL SEMESTER 2024-2025

SLOT: E1

3.	Explore the given scenario of a network with IDS and IoT. Explain the IDS in the scenario and write about the different types of intrusion detection in this network.  	10
4.	*WannaCry* exploited a vulnerability in Microsoft Windows that allowed it to spread from one infected system to others on the same network. Once a system was infected, WannaCry encrypted the victim's files and demanded a payment. It spread globally, infecting hundreds of thousands of computers in over 150 countries, including hospitals, universities, and businesses. In some cases, the attack disrupted entire organizations, preventing them from accessing important data and files. What is the above malware attack called? Explain the steps to prevent these malware attacks.	10
5.	Grey box testing is one of the software testing technique that enables the test of a software product. This Grey box testing has been executed to the target Ip address 192.168.1.187. The complete process has been executed upon the Kali Linux machine. Identify the vulnerabilities and risks involved in the above Pen testing. Explain the steps to encounter those vulnerabilities in Linux OS.	10

****