Air University

Student ID 237285

Final Semester Examinations: Fall 2025

Subjective Part
(To be solved on Answer Books only)

Subject: Parallel and Distributed Computing
Class: BSCYS
Section(s): V-A&B
Course Code: CS-426

Time Allowed: 3 hours
Max Marks: 100
FM's Name: Eman Munir
FM's Signature:

INSTRUCTIONS

- Attempt responses on the answer book only.
- Nothing is to be written on the question paper.
- Rough work or writing on question paper will be considered as use of unfair means.

		Marks
	Q. No. 1 (CLO 3)	
	A cybersecurity analytics team is processing a large intrusion log file on a multi-core server. Initially, the analysis tool runs sequentially and takes several hours to finish. The team decides to use OpenMP to speed up the process. The log file consists of independent entries, and each entry must be checked for suspicious patterns. a) Explain why OpenMP is suitable for this problem based on the OpenMP programming model. b) Describe how the Fork–Join execution model of OpenMP would work in this scenario. c) Identify which data in this scenario should be shared and which should be private, and justify your choice. d) Give one reason why the compiler alone may fail to parallelize this code automatically, making OpenMP necessary.	10+5+5+5
	Q. No. 2 (CLO 2 &3)	
	A research team is simulating a distributed brute-force password attack using thousands of processors. All processors need to read the same password policy file, but only one processor is allowed to update the global "password found" flag. a) Which PRAM model (EREW, CREW, or CRCW) best represents this situation? Explain why. b) Identify which memory accesses are concurrent reads and which are exclusive writes. c) Explain how synchronization is handled in the chosen PRAM model. d) Why would the RAM model be unsuitable for this scenario?	10+5+5+5
	Q No. 3 (CLO 4)	

	During a large-scale DDoS attack, several processing nodes in a security system become overloaded and fail The system must continue to operate and provide accurate alerts to administrators. a) Explain how Group Masking would handle node failures during the attack. b) Explain how Hierarchical Masking would handle the same failures. c) Compare both techniques in terms of response time, resource usage, and fault isolation. d) Conclude which approach is more appropriate during sustained cyber attacks and justify your answer.	5+5+5+5
	Q No. 4 (CLO 1&2)	
	A shared-memory intrusion detection system (IDS) runs on a multi-core server and processes network traffic in parallel. Each thread performs packet inspection and updates a global threat counter whenever suspicious activity is detected. During heavy traffic: • Some threads finish quickly while others are delayed • The threat counter shows inconsistent values • CPU usage appears high, but detection speed does not improve The development team claims that using multiple threads automatically guarantees better performance. a) Identify two scheduling-related issues that could explain why high CPU usage does not lead to better detection performance. Explain your reasoning. b) Explain how improper synchronization can lead to inconsistent threat counter values, even if all threads are running correctly. c) Discuss how poor scheduling decisions can amplify synchronization problems in this system. d) State one design improvement related to scheduling and one related to synchronization that would improve system reliability.	10+10+5+5

**********End of Question Paper**********