GYANMANJARI INNOVATIVE UNIVERSITY

GYANMANJARI INSTITUTE OF TECHNOLOGY

M. Tech.-End Semester Examination (ESE)- Summer-2026

Enrollment No.: _____

Subject Code: METCS12512 **Date: 21-05-2026**

Subject Name: Artificial Intelligence in Cyber Security -II **Semester: 02**

Time: 10:30 AM to 01:30 PM **Total Marks: 100**

Instructions:

1. **Question No. 1 is compulsory.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

			Marks
Q.1	(a)	Explain the cyber threat landscape and the concept of the cyber attacker's economy.	10
	(b)	Describe intrusion detection using heuristics and data-driven methods.	10
Q.2	(a)	Explain the theory of network defense and its components.	10
		OR	
	(a)	Explain monetization strategies in the consumer web.	10
	(b)	Analyze adversarial machine learning and its importance in cyber security.	10
		OR	
	(b)	Summarize recent trends in AI for cyber security and propose future directions.	10
Q.3	(a)	Compare supervised, semi-supervised, and unsupervised learning in network security.	10
	(b)	Explain bot activity detection using supervised learning.	10
		OR	
Q.3	(a)	Evaluate poisoning attacks and defenses in machine learning models.	10
	(b)	Compare cold start vs warm start problems in machine learning models.	10
Q.4	(a)	Analyze the limitations of machine learning in security systems.	10
	(b)	Analyze unsupervised machine learning algorithms for anomaly detection.	10
		OR	
Q.4	(a)	Compare density-based methods and statistical metrics for anomaly detection.	10
	(b)	Explain the process of feature extraction from network traffic captures.	10
Q.5	(a)	Analyze false positives and false negatives in abuse detection systems.	10
	(b)	Evaluate evasion attacks with suitable examples and defenses.	10
		OR	
Q.5	(a)	Explain host-based and network-based intrusion detection systems.	10
	(b)	Explain the iterative approach used in spam fighting using machine learning.	10