U.S.N.										

B.M.S. College of Engineering, Bengaluru-560019

Autonomous Institute Affiliated to VTU

January / February 2025 Semester End Main Examinations

Programme: B.E. **Semester: VII**

Branch: Artificial Intelligence and Machine Learning **Duration: 3 hrs.**

Course Code: 24AM7PEACY **Max Marks: 100**

Course: AI for Cyber Security

Instructions: 1. Answer any FIVE full questions, choosing one full question from each unit.
2. Missing data, if any, may be suitably assumed.

Important Note: Completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages. Revealing of identification, appeal to evaluator will be treated as malpractice.

		UNIT - I	CO	PO	Marks
1	a)	Discuss the evolution of Artificial Intelligence (AI) from expert systems to data mining, providing examples in each stage.	CO1	PO1	**08**
	b)	Explain the significance of expert systems in the development of AI, highlighting their strengths and limitations.	CO2	PO1	**06**
	c)	With suitable examples explain the indeterministic nature of reality that influence AI models.	CO1	PO1	**06**
		OR			
2	a)	Describe the process of mining data for models in the context of AI, including data preprocessing and feature selection for applying in Cybersecurity.	CO1	PO1	**08**
	b)	Compare and contrast expert systems and machine learning, focusing on their methodologies and applications.	CO2	PO2	**06**
	c)	Identify the challenges of AI in providing Cybersecurity.	CO1	PO1	**06**
		UNIT - II			
3	a)	Explain how a Perceptron can be used to detect spam. Provide a simple example and outline the steps involved.	CO2	PO1	**08**
	b)	Identify the pros and cons of using Perceptron for spam detection and suggest improvements.	CO2	PO1	**06**
	c)	Analyse how a linear classifier work in the context of spam filters with suitable example.	CO2	PO2	**06**
		OR			
4	a)	Elucidate the Support Vector Machine optimization strategy for spam detection, and provide a practical example.	CO2	PO1	**08**

		b)	Explain the process of phishing detection using logistic regression, detailing the key steps.	*CO2*	*PO1*	**06**
		c)	With suitable example explain the role of decision trees in phishing detection.	*CO2*	*PO2*	**06**
			UNIT - III			
	5	a)	Outline the various malware detection strategies.	*CO1*	*PO1*	**08**
		b)	Describe the methodology of static malware analysis, and explain its significance.	*CO1*	*PO1*	**05**
		c)	Identify the challenges faced during static malware analysis. Provide solutions to overcome the challenges.	*CO2*	*PO2*	**07**
			OR			
	6	a)	Explain the tools and techniques used in dynamic malware analysis, providing examples of each.	*CO1*	*PO1*	**08**
		b)	Write a note on the following with suitable examples with respect to malware analysis: i) Botnets ii) Disassemblers	*CO1*	*PO1*	**05**
		c)	Describe the anti-analysis tricks used by malware to evade detection, and suggest countermeasures.	*CO2*	*PO2*	**07**
			UNIT - IV			
	7	a)	Describe the network anomaly detection techniques used in cybersecurity, and their importance.	*CO1*	*PO1*	**08**
		b)	Differentiate between Host Intrusion Detection Systems and Network Intrusion Detection Systems.	*CO2*	*PO2*	**05**
		c)	"Service logs can be turned into datasets for anomaly detection". Justify the statement and provide a step-by-step approach.	*CO3*	*PO3*	**07**
			OR			
	8	a)	Explain the importance of securing user authentication in cybersecurity and the common challenges faced.	*CO1*	*PO1*	**08**
		b)	Exemplify the common practices to prevent authentication abuse.	*CO2*	*PO2*	**05**
		c)	Explain the process of detecting fake logins into the user accounts.	*CO3*	*PO1*	**07**
			UNIT - V			
	9	a)	Explain the fraud detection algorithms used in cloud AI solutions and their applications.	*CO2*	*PO1*	**08**
		b)	Compare expert-driven predictive models and data-driven predictive models, highlighting their advantages and disadvantages.	*CO2*	*PO2*	**07**

		c)	Elucidate how machine learning can be used in credit card fraud detection.	*CO1*	*PO1*	**05**
			OR			
	10	a)	Describe the best practices for designing a Fraud Detection and Prevention System (FDPS), providing detailed steps.	*CO2*	*PO2*	**08**
		b)	Explain how FDPS combines expert-driven and data-driven models, and their complementary benefits.	*CO2*	*PO1*	**07**
		c)	Identify the possible credit card fraud scenarios where credit card information can be compromised.	*CO1*	*PO1*	**05**

****