Roll No. : .....

Galgotias College of Engineering and Technology, Greater Noida

Pre University Test (PUT) : Odd / Even Semester 2024 - 2025

Course/Branch : **AI&DS**
Subject Name : **Machine Learning & Network Security**
Subject Code : **KAD075**
Semester : **7th**
Max. Marks : **100**
Time : **180 min**

CO-1 *: Learn different machine learning algorithms to secure information.*
CO-2 *: Implement filtering methods using machine learning techniques.*
CO-3 *: Analyze different methods of detecting anomalies.*
CO-4 *: Perform malware analysis using extracted information.*
CO-5 *: Visualize the attacks on consumer websites. And model machine learning-based systems to create production environments.*

Section – A # 20 Marks (Short Answer Type Questions)

Attempt **ALL** the questions. Each Question is of 2 marks (10 x 2 = 20 marks)

Q. No.		COx	Question Description # Attempt ALL the questions. Each Question is of 2 marks
1	a	CO1	List two real-world applications of machine learning in network security. (BKL : K1 Level)
	b	CO1	Explain the iterative approach used in spam fighting and why it is considered effective? (BKL : K2 Level)
	c	CO2	Define anomaly detection. Explain how it is different from supervised learning. (BKL : K1 Level).
	d	CO2	Explain the purpose of building a predictive model for classifying network attacks. (BKL : K2 Level)
	e	CO3	List two features commonly used in malware detection. (BKL : K1 Level)
	f	CO3	Describe how clustering helps in identifying patterns of abuse. (BKL : K2 Level)
	g	CO4	Define target recognition in the context of machine learning. Provide an example of its application. (BKL : K1 Level)
	h	CO4	Discuss how image recognition is used in security applications with one example. (BKL : K2 Level)
	i	CO5	Explain the What is meant by machine learning system maturity. (BKL : K2 Level)
	j	CO5	List two factors that affect the quality of data in machine learning systems. (BKL : K1 Level).

Section – B # 30 Marks (Long / Medium Answer Type Questions)

Attempt **ALL** the questions. Each Question is of 6 marks (5 x 6 = 30 marks)

Q.2 (CO-1) : Illustrate how machine learning can be integrated into existing network security frameworks. Highlight the benefits and challenges of such integration. (BKL : K3 Level)

OR

Compare the effectiveness of traditional methods versus machine learning techniques in detecting and mitigating cyber threats. (BKL : K4 Level)

Q.3 (CO-2) : Apply heuristic methods for intrusion detection to explain how rule-based systems can identify abnormal network behavior. Provide an example. (BKL : K3 Level)

OR

Illustrate the steps involved in feature engineering for an anomaly detection model. Explain how specific features contribute to improving accuracy. (BKL : K3 Level)

Q.4 (CO-3) : Apply feature generation techniques to create a dataset for malware classification. Explain how these features can help differentiate between benign and malicious software. (BKL : K3 Level)

OR

Explain the role of supervised learning in detecting abuse on the consumer web. Explain how it improves the accuracy of abuse detection systems. (BKL : K3 Level)

Q.5 (CO-4) : Compare and contrast different methods of detecting anomalies in network traffic, such as clustering, statistical methods, and machine learning-based approaches. Discuss their strengths and weaknesses. (BKL : K4 Level)

OR

Describe how attack visualizations on consumer websites can aid in threat detection and response. Explain how machine learning algorithms can enhance the process of attack visualization? (BKL : K3 Level)

Q.6 (CO-5) :Describe the key considerations for ensuring the maintainability of a machine learning model in a production environment. Discuss how do these considerations impact the model's long-term success. (BKL : K3 Level)

OR

Discuss the relationship between data quality and model performance in machine learning systems. Discuss how poor data quality can impact the effectiveness of machine learning models, and what step-scan be taken to ensure data quality? (BKL : K4 Level)

Section – C # 50 Marks (Medium / Long Answer Type Questions)

Attempt **ALL** the questions. Each Question is of 10 marks.

Q.7 (CO-1) : Attempt any TWO question. Each question is of 5 marks.

a. Explain the concept of the cyber threat landscape. Explain how machine learning has been integrated into the evolution of cybersecurity to address emerging threats. (BKL : K3 Level)

b. Evaluate the role of machine learning in spam detection. Explain how does the iterative learning process in spam filters help in improving accuracy and reducing false positives. (BKL : K5 Level)

c. Describe how machine learning algorithms are used in real-world security applications. Provide two examples of how machine learning has been effectively applied in combating cyber threats. (BKL : K3 Level)

Q.8 (CO-2) : Attempt any TWO question. Each question is of 5 marks.

a. Identify the key challenges of using machine learning for anomaly detection in real-time systems. Explain how issues such as class imbalance, concept drift, and high false positives can be addressed. (BKL : K4 Level)

b. Compare and contrast anomaly detection and supervised learning. Explain how these two methods differ in the context of network traffic analysis, and in what scenarios would one be preferred over the other. (BKL : K4 Level)

c. Design a predictive model for classifying network attacks. Discuss the steps involved in building the model, including data collection, feature selection, algorithm choice, and model evaluation. (BKL : K5 Level)

Q.9 (CO-3) : Attempt any Two question. Each question is of 5 marks.

a. Discuss the differences between live and dead malware analysis. Discuss how both approaches contribute to a comprehensive understanding of malware behavior. (BKL : K4 Level)

b. Explain the challenges of analyzing Android malware. Explain how the unique characteristics of Android devices make malware analysis more difficult compared to traditional systems? (BKL : K4 Level)

c. Examine how clustering techniques can be used to detect abuse on the consumer web. Discuss how does clustering help identify patterns of behavior that might be missed by traditional rule-based systems. (BKL : K4 Level)

Q.10 (CO-4) : Attempt any TWO question. Each question is of 5 marks.

a. Explain how filtering methods can be implemented to detect malicious activities in network traffic. List the advantages of using machine learning-based filtering techniques over traditional rule-based methods. (BKL : K3 Level)

b. Compare and contrast different methods of detecting anomalies in network traffic. Discuss the strengths and limitations of methods such as clustering, classification, and statistical analysis for detecting network anomalies. (BKL : K4 Level)

c. Evaluate the use of target recognition in security applications. Explain how machine learning contribute to target recognition in areas such as surveillance, military, or cyber defense. (BKL : K4 Level)

Q.11 (CO-5) : Attempt any TWO question. Each question is of 5 marks.

a. Discuss the importance of model performance in a production environment. Discuss metrics would you use to assess the model's effectiveness, and why are they crucial for maintaining model reliability. (BKL : K3 Level)

b. Examine the role of monitoring and alerting systems in machine learning production environments. Explain how these systems help in maintaining the quality and reliability of deployed models. (BKL : K4 Level)

c. Evaluate the impact of data quality on the performance of machine learning models in production systems. Mention the strategies that can be used to improve performance. (BKL : K4 Level)

==========