Roll No: | | | | | | | | | | | |

PRESIDENCY UNIVERSITY

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

Presidency University Act, 2013 of the Karnataka Act No. 41 of 2013 | Established under Section 2(f) of UGC Act, 1956
Approved by AICTE, New Delhi | Approved By BCI
Bengaluru

Mid Term Examinations - October 2026

Date: 05/10/2026 **Time:** 11:45 AM - 01:15 PM

Course Code: CBC3407 **Course Name:** Machine Learning for Cyber Threat Detection

Semester: Seventh Semester **Max. Marks:** 50 **Weightage:** 50%

CO - Levels	CO1	CO2
Marks	44	46

PART A: Answer Following Questions. 10 M

Q.N.	Questions	M	CO	BT
1	Define cybersecurity.	2	CO1	BT1
2	What is a cyber threat? Give one example.	2	CO1	BT1
3	Define machine learning-based threat modeling.	2	CO2	BT2
4	What is supervised learning? Give one cybersecurity application.	2	CO2	BT1
5	Differentiate between classification and regression.	2	CO2	BT2

PART B : Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
6	Explain the cyber threat landscape and analyze the major types of cyber threats, including phishing, malware, DoS, and ransomware, with suitable examples.	10	CO1	BT2
7	Explain the scope and opportunities of machine learning in cybersecurity. Discuss its applications in detecting and preventing cyber threats with suitable examples.	10	CO1	BT2

PART C: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
8	Explain Indicators of Compromise (IoCs), their types, and their role in identifying cybersecurity incidents. Illustrate how IoCs can be used to investigate a suspected cyberattack.	10	CO1	BT2
9	Compare signature-based and anomaly-based intrusion detection systems. Discuss their working principles, advantages, limitations, and suitability for detecting known and unknown attacks.	10	CO1	BT2

PART D: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
10	Explain the role of machine learning in threat modeling. Describe the major stages involved in developing an ML-based threat detection system with a suitable cybersecurity example.	10	CO2	BT2
11	Explain supervised and unsupervised learning. Compare their working principles, requirements, advantages, and applications in cybersecurity.	10	CO2	BT2

PART E: Answer Any 1 Following Questions. 10 M				
Q.N.	**Questions**	**M**	**CO**	**BT**
12	A network traffic dataset contains source and destination IP addresses, protocol, packet size, flow duration, and packet rate. Analyze these features and propose a suitable feature selection strategy for detecting DoS attacks.	10	CO2	BT4
13	Analyze the impact of missing values, duplicate records, inconsistent values, and unscaled features on the quality of a network traffic dataset, and examine how appropriate data preprocessing techniques can address these issues to improve machine learning model performance.	10	CO2	BT4