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

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

PRESIDENCY UNIVERSITY

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: 06/10/2026 **Time:** 02:00 PM - 03:30 PM

Course Code: CCS3403 **Course Name:** AI and ML in Cyber Security

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

CO - Levels	CO1	CO2
Marks	46	44

PART A: Answer Following Questions. 10 M

Q.N.	Questions	M	CO	BT
1	Explain the role of classification in threat intelligence.	2	CO1	BT2
2	Justify why phishing detection can be formed as a regression task.	2	CO1	BT2
3	Determine real world relevance of XGBoost model in cyber security.	2	CO1	BT2
4	How to solve the botnet expansion rate prediction problem?	2	CO2	BT3
5	Determine how ML algorithms can be used to predict Data Exfilitration Volumes.	2	CO2	BT3

PART B : Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
6	**A.** Sketch the workflow of **Anomaly Detection** using unsupervised Learning. **[4 Marks]** **B.** Illustrate the **K-Means Clustering Algorithm** and List the limitations.	10	CO2	BT4
7	**A.** Emphasise on the role of **Unsupervised Learning** in **Allert Triage. [5 Marks]** **B.** Determine the importance of **ML Models in Domain Generation Algorithms. [5 Marks]**	10	CO2	BT4

PART C: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
8	**A.** Give an overview of the advantages of **ML Methods** in **Vulnarability Management** over **CVSS** based traditional methods. **[5 Marks]** **B.** Determine the advantages of **Supervised Learning** in **Attack Prevention and Autonomous Defence. [5 Marks]**	10	CO1	BT4
9	**A.** Evaluate the process by which **Google** performs its **Phishing and Spam Detection** Tasks using ML. **[6 Marks]** **B.** Evaluate the role of **Classification** in real world **Behaviour Analysis** by **Next Generation Antiviruses. [4 Marks]**	10	CO1	BT4

PART D: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT

10	**A.** Identify the limitations of **Atomic Static Analysis** and elaborate the effectiveness of **Context-Based Detection** using **ML Models. [5 Marks]** **B.** Determine the necessity of **Hybrid Detection Mechanism** in **Threat Perception and User Behaviour Analytics. [5 Marks]**	10	CO1	BT2
11	**A.** Provide a complete **Mapping** of the **Cyber Kill Chain Methodology Steps** with the corresponding and relevant **Machine Learning Methods,** and list one widely used **Algorithm** for the same. **[3+2 Marks]** **B.** Briefly describe a **Machine Learning Life Cycleb** with a neat diagram. **[3+2 Marks]**	10	CO1	BT2

PART E: Answer Any 1 Following Questions. 10 M				
Q.N.	**Questions**	**M**	**CO**	**BT**
12	**A.** Explain the different **ML methods** can be used to perform **Signature Based Detection** in the context of **Hashing and Byte-Sequence Signatures. [5 Marks]** **B.** Explain how **Behaviour Based Detection** can be framed as an **Anomaly Detection** task and effectiveness of **UNsupervised Learning** for the same. **[3+2 Marks]**	10	CO2	BT2
13	**A. Justify** how **Malware Type Detection** can be viewed as both a **Supervised or Unsupervised ML Task[5 Marks]**. **B.** Discuss the **Data Imballance** problem in **ML** tasks for Cyber Security and **Define the Processes** that can be used to solve this problem.	10	CO2	BT2