MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
(A constituent unit of MAHE, Manipal)

II SEMESTER M.TECH. (CSIS) (DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING) MAKEUP SEMESTER EXAMINATIONS, MAY 2024

SUBJECT: AI AND ML TECHNIQUES IN CYBER SECURITY (CSE - 5416)

REVISED CREDIT SYSTEM

(XX/XX/2024)

Time: 9:30 am to 12:30 pm MAX.MARKS: 50

INSTRUCTIONS TO CANDIDATES:-

- Answer **ALL** the questions.
- Missing data may be suitable assumed.

		Marks
1A.	Discuss some of the principal threats in cyber security.	5M
1B.	Explain the different types of malwares.	3M
1C.	List some of the disadvantages of k-means clustering algorithm.	2M
2A.	For the given Dataset 1, find the best prediction algorithm. Justify your answer.	4M

	accountAgeDays	numItems	localTime	paymentMethod	paymentMethodAgeDays	label
31442	2000	1	4.748314	storecredit	0.000000	0
27232	1	1	4.886641	storecredit	0.000000	1
8687	878	1	4.921349	paypal	0.000000	0

Dataset 1

2B.	List and discuss the improvements to basic gradient boosted decision tree to better perform, better generalize and more efficient model.	3M
2C.	Discuss the different ways to construct training data to evaluate your model.	3M
3A.	Explain the concept of osquery with example.	4M
3B.	Discuss the different understanding of malware classification.	4M
3C.	List and explain the important features of standard HTTP server log file.	2M
4A.	Describe the different categories of active attacks.	4M
4B.	Is machine learning algorithm model code or data? Justify with a suitable answer.	3M
4C.	Discuss the issue of hyperparameters in model quality and provide a solution to optimize the hyperparameter.	3M
5A.	Describe the different dimensions of properties for qualitatively analyzing attacks on adversarial machine learning systems.	5M
5B.	Discuss the significant benefits to designing online learning systems that behave like an offline batch system. Also discuss the different ways to detect poisoning attack.	3M
5C.	Describe the different features that are indicative of financial fraud.	2M