SARVAJANIK UNIVERSITY
Sarvajanik College of Engineering and Technology
Master of Technology

Year: M. Tech. I (Semester - II)

Subject Name: AI-ML techniques for security **Subject Code:** MTCO24201
Type of course: Professional Elective-III
Prerequisite (if any): Artificial Intelligence, Machine Learning, Security

List of Courses where this course will be prerequisite: --

Rationale: Machine learning is a method of data analysis that automates analytical model building. It is a branch of artificial intelligence based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention. This subject will help students to detect anomalies, conduct malware analysis, uncover attackers within the network by finding patterns, examine how attackers exploit consumer-facing websites, and understand the threat attackers pose to machine learning solutions.

Teaching and Examination Scheme:

Teaching Scheme				Theory Marks			Practical Marks		Total
L	T	P	C	TEE	CA1	CA2	TEP	CA3	
3	0	2	4	60	25	15	30	20	150

CA1: Continuous Assessment (assignments/projects/open book tests/closed book tests CA2: Sincerity in attending classes/class tests/ timely submissions of assignments/self-learning attitude/solving advanced problems TEE: Term End Examination TEP: Term End Practical Exam (Performance and viva on practical skills learned in course) CA3: Regular submission of Lab work/Quality of work submitted/Active participation in lab sessions/viva on practical skills learned in course

Content:

Sr. No.	Content	Total Hrs
1	Machine Learning and Security: Cyber Threat Landscape, The Cyber Attacker's Economy - A Marketplace for Hacking Skills, Indirect Monetization, The Upshot, What Is Machine Learning? - What Machine Learning Is Not, Adversaries Using Machine Learning, Real-World Uses of Machine Learning in Security, Spam Fighting: An Iterative Approach, Limitations of Machine Learning in Security	5
2	Machine Learning Preliminaries: Supervised Learning - Regression, Classification, Supervised Learning in Adversarial Settings, Unsupervised	5

	Learning - Clustering, Unsupervised Learning in Adversarial Settings, Reinforcement Learning - Reinforcement Learning in Adversarial Settings	
3	Anomaly Detection: When to Use Anomaly Detection against Supervised Learning, Intrusion Detection with Heuristics, Data-Driven Methods, Feature Engineering for Anomaly Detection, Anomaly Detection with Data and Algorithms, Challenges of Using Machine Learning in Anomaly Detection, Response and Mitigation, Practical System Design Concerns	6
4	Malware Analysis: Understanding Malware - Defining Malware Classification, Feature Generation - Data Collection, Generating Features, Feature Selection, From Features to Classification - How to Get Malware Samples and Labels	6
5	Network Traffic Analysis: Theory of Network Defense, Machine Learning and Network Security, Building a Predictive Model to Classify Network Attacks	5
6	Protecting the Consumer Web: Monetizing the Consumer Web, Types of Abuse and the Data That Can Stop Them, Supervised Learning for Abuse Problems, Clustering Abuse, Further Directions in Clustering	5
7	Adversarial Machine Learning: Terminology, The Importance of Adversarial ML, Security Vulnerabilities in Machine Learning Algorithms, Attack Technique: Model Poisoning, Attack Technique: Evasion Attack	5
8	Machine Learning in Privacy Preserving: An Introduction to Privacy-Preserving Data Publishing, An Introduction to Privacy-Preserving Data Mining, Need for Privacy Preservation, Applications of Privacy Preservation, Techniques for Privacy Preserving Data Mining - k-anonymity, l-diversity	5
9	AI and Machine Learning in Cyber security: What AI/ML can do for cyber security?, How AI/ML is used in cyber security?, Examples of machine learning in cyber security, The future of cyber security	3

Reference Books:

Sr.No.	Title of book /article	Author(s)	Publisher and details like ISBN	Year of publication	Publication Edition
1	Machine Learning & Security	Clarence Chio, David Freeman	O'Reilly Media, Inc.	Latest Edition	Latest Edition

			ISBN: 9781491979907		
2	Privacy-Preserving Data Mining Models and Algorithms-	Editors: Aggarwal, Charu C., Yu, Philip S.	Springer, 978-0-387-70992-5	Latest Edition	Latest Edition
3	Introduction to Privacy-Preserving Data Publishing: Concepts and Techniques	Benjamin C.M. Fung, Ke Wang, Ada Wai-Chee Fu, Philip S. Yu	CRC Press, Taylor & Francis Group	Latest Edition	Latest Edition
4	Adversarial Machine Learning	Editors: Aneesh Sreevallabh Chivukula, Xinghao Yang, Bo Liu, Wei Liu, Wanlei Zhou	Springer International Publishing	Latest Edition	Latest Edition
5	Machine Learning for Computer and Cyber Security Principles, Algorithms, and Practices	Editors: Brij B. Gupta, Michael Sheng	CRC Press	Latest Edition	Latest Edition
6	Hands-On Machine Learning for Cybersecurity	Soma Halder, Sinan Ozdemir	Packt	Latest Edition	Latest Edition

Course Outcomes:

Sr. No.	CO statement	Marks % weightage
CO-1	Explore the fundamental concepts of machine learning for devising security mechanisms in Adversarial Settings.	23

CO-2	Detect anomalies, including breaches, fraud, and impending system failure	13
CO-3	Explore the usage of machine learning techniques for malware analysis, network traffic analysis, and cyber security	31
CO-4	Examine how attackers exploit consumer-facing websites and app functionality.	11
CO-5	Analyze the machine learning approaches for security for probable abuse by the adversary.	11
CO-6	Integrate privacy-preservation in data publishing and data mining with the help of various techniques for different applications.	11

List of Open learning website:

- https://aaai18adversarial.github.io/index.html

List of Open Source Software:

- Python
- OpenCV
- Pytorch

FOR LAB SESSIONS:

List of Experiments:

Minimum 10 Experiments are to be designed covering various experimental activities covering the content of this subject from different domains