

 SANKALCHAND PATEL UNIVERSITY ॥ अथातो ज्ञानजिज्ञासा ॥	Faculty of Engineering and Technology Master of Technology (Semester II / First year) In Effect from Academic Year 2023-24
--	---

Branch Name:	CYBER SECURITY
Program Code:	ET207
Course Title:	Artificial Intelligence and Machine Learning for Cyber Security Practical
Course Code	2ET2070201P
Pre-requisite Course:	The main objective of this practical session is that students will get the exposure to various Machines learning tools context of cyber security.

Course Objectives: The objective of this course is to learn and develop an inclusive understanding of Artificial Intelligence and machine learning for exceptional security challenges.

Teaching and Examination Scheme:

Credit	Teaching Scheme Hours per week				Evaluation Scheme (Marks)								Total (Marks)
					Theory (Marks)				Practical (Marks)				
	L	T	P	Total	SEE		CCA		SEE		CCA		
					Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.	
1	-	-	2	2	-	-	-	-	10	25	10	25	50

Course Contents:

Unit	Details	Contact Hours
1	a. Implement an algorithm to demonstrate the significance of genetic Algorithm. b. Implement linear regression using python. c. Implement k-nearest neighbors' classification using python.	8
2	a. Implement Naïve Bayes Classification in Python. b. Develop Logistic Regression Model for a given dataset. c. Build Artificial Neural Network model with back propagation on a given dataset.	8
3	a. Make use of Data sets in implementing the machine learning algorithms b. Implement the machine learning concepts and algorithms in any suitable language of choice. c. Write a program to implement the naïve Bayesian classifier for a sample training data set stored as a .CSV file. d. Write a Python program to demonstrate various Data Visualization Techniques.	8

4	a. Find the practical solutions for classification and regression approaches in real-world applications.(Any application.) b. Write a Python program to demonstrate various Data Visualization Techniques.	8
---	---	---

Reference Books:

1. Hands-On Machine Learning for Cyber security: Safeguard Your System by Making Your Machines Intelligent Using the Python Ecosystem.
2. Machine Learning for Cyber security Cookbook: Over 80 Recipes on how to implement Machine Learning Algorithms for Building Security Systems Using Python.

Course Outcomes:

At the end of the course, students will be able to:

Course Outcomes	Description	Bloom's Taxonomy Level
CLO1	Learn and understand what Machine learning is, including all the tools of the trade. Understand that linear algebra powers most ML.	Understanding (2)
CLO2	Supervised learning, requirement for labeled data, using a loss function to guide the optimization.	Applying (3)
CLO3	Learn to conduct anomaly detection, spam classification, automated malware classification. Security oriented machine learning tasks.	Applying (3)
CLO4	Fundamentals of classification, decision trees, logistic regression, Neural networks.	Applying (3)

Mapping of CLO with PO and PSO

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes(PSOs)			
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3	PS O4
CLO1	H	M	M		H											
CLO2	H	H			M											
CLO3	H	M	M		H											
CLO4	M	M	M		H							L				

H: High, M: Medium, L: Low