

Branch Name:	CYBER SECURITY
Program Code:	ET207
Course Title:	Artificial Intelligence and Machine Learning for Cyber Security
Course Code:	2ET2070201T
Pre-requisite Course:	Able to attain a thorough knowledge in the area of Privacy and Storage security and related Issues

Course Objectives: After successful completion of the course, student will be able to

1. To learn about preparing the data for machine learning, common machine learning techniques and tools (supervised learning, unsupervised learning, deep learning, and large-scale data analysis), and their applications to cyber security.
2. Using Artificial Intelligence Tools to Enhance Security
3. Politics and Big data and Decision Making Process
4. Artificial Intelligence in Politics
5. The Future of AI in Advancing Security and Promoting

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.	
3	3	-	-	3	24	60	16	40	-	-	-	-	100

Course Contents:

Unit No	Topics	Total Hours	Weight age (%)
1	Basics of Machine Learning in Cyber security : Definitions of machine learning and use cases, Delving into machine learning in the cyber security world, Different types of machine learning systems, Different data preparation techniques, Machine learning architecture, A more detailed look at statistical models and machine learning models, Model tuning to ensure model performance and accuracy, Machine learning tools.	10	25
2	Knocking Down CAPTCHAs : Characteristics of CAPTCHAs, Using artificial intelligence to crack CAPTCHAs Types of CAPTCHA, Solving CAPTCHAs with neural networks.	08	15
3	AI for Cyber security : Applying AI in cyber security, The evolution from expert systems to data mining and AI, The different forms of automated learning, The characteristics of algorithm training and optimization, Beginning with AI via Jupyter Notebooks, Introducing AI in the context of cyber security.	10	25
4	Detecting Cyber security Threats with AI : How to detect spam with Perceptrons Image spam detection with support vector machines (SVMs), Phishing detection with logistic regression and decision trees Spam detection with Naive Bayes, Spam detection adopting NLP.	09	15
5	AI for Cyber security Arsenal: Classification Regression, Dimensionality reduction, Clustering, Speech recognition Video anomaly detection, Natural language processing (NLP), NLP, Large-scale image processing, Social media analysis.	09	20

Text Books:

1. Tom M Mitchell, Machine Learning, McGraw Hill, 1997
2. Jake Vanderplas, Python Data Science Handbook, O'Reilly Media, 2016

Reference Books:

1. Dr. Nilakshi Jain (2019). Artificial Intelligence, As per AICTE: Making a System Intelligent, Wiley Publication
2. McKinney, W Brij B. Gupta and Quan Z. Sheng.(2019). Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices (Cyber Ecosystem and Security), CRC Press Publication

Course Learning Outcomes (CLO):

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) Applying (3)
CLO2	Explain the basic concepts and the limitations of Artificial Intelligence.	Applying (3)
CLO3	Understand, identify, and evaluate the limitations and risks associated with applying machine learning algorithms to cyber security.	Applying (3)
CLO4	Broad understanding of different cyber security tasks/problems, for which, a AI learning technique can be applied;	Applying (3)
CLO5	Model validation and evaluation. Gain the skill of plotting both learning curves and model evaluation curves. Ascertain whether more complexity is required or more data.	Applying (3)

Mapping of CLO with PO and PSO

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes(PSOs)			
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4
CLO1	H	M	M													
CLO2	H	H	M		M							L				
CLO3	H	H	M		M											
CLO4	M	M	M		M											

H: High, M: Medium, L: Low