

Branch Name:	Computer Engineering
Program Code:	ET103
Semester/Year:	Semester V / Third Year
Subject Title:	Machine Learning for Cyber Security [Specialization in Cyber Security]
Subject Code:	2ET1030509T
Prerequisite:	Introduction to Linear Algebra and have basic familiarity with probability theory.

Course Objective:

- Learn the concept of Machine learning
- Understand basic theory of classification and regression techniques
- Get basic hands on experience with supervised, unsupervised learning methods
- Understand and implement machine learning algorithms and models for Cyber Security problems such as malware analysis, intrusion detection, spam filtering, fraud detection, online behavior analysis etc

Teaching Scheme (Hours per week)					Evaluation Scheme (Marks)								
Credit	L	T	P	Total	Theory (Marks)				Practical (Marks)				Total (Marks)
					SEE		CCA		SEE		CCA		
					Min	Max	Min	Max	Min	Max	Min	Max	
3	3	-	-	3	24	60	16	40	-	-	-	-	100

Subject Contents			
Sr. No	Topic	Total Hours	Weightage (%)
1	Introduction to Machine Learning: What is human learning? What is Machine Learning? Human learning versus machine learning, Types of machine learning, Applications of machine learning to network security, Tools for machine learning.	06	15
2	Preparing to Model , Feature Engineering: Machine Learning activities, Basic Types of data in Machine Learning, Structures of data, Data Quality and Remediation, Data Pre-Processing, Introduction to Feature Engineering, Feature Transformation, Feature Subset Selection, regression	06	15
3	Introduction to adversarial machine learning, threat models, Defending against adversaries, Modelling and Evaluation: Selecting a Model, Training a Model, Model Representation and Interpretability, Evaluating Performance of a Model, Improving Performance of a Model	06	15
4	Fairness, Transparency, and Explainability in cybersecurity ML models : Privacy definitions and how to actualize privacy for cybersecurity applications in industry Externalities and implications of errors in ML models for cybersecurity	04	15
5	Malware Analysis : Static and Dynamic Analysis, Models that work well Spam/Phishing Detection : Training Models and Measuring Efficacy Network Intrusion Detection	06	20
6	Fraud Detection, Machine Learning Models for Outlier detection, DDoS Detection, Models with Statistical regression combined with distance metric	05	20

Text-books:

1. Tom Mitchell. Machine Learning. McGraw Hill, 1997
2. Artificial Intelligence and Data Mining Approaches in Security Frameworks Editor(s):Neeraj Bhargava, Ritu Bhargava, Pramod Singh Rathore, Rashmi Agrawal, 2021.

References:

1. Peter Harrington, "Machine Learning in Action", DreamTech
2. Michael Bowles, "Machine Learning in Python", Wiley
3. Gavin Hackling, Mastering Machine Learning with scikit-learn, Packt
4. Jake Vanderplas, Python Data Science Handbook, O'Reilly Media, 2016

List of Open Source Software/learning website:

1. <https://github.com/jivoi/awesome-ml-for-cybersecurity>
2. <https://www.techtarget.com/>

Course Learning Outcomes (CLO): On completion of this course, the students will be able to:

CLO	Description	Bloom's Taxonomy Level
COL1	Understanding the fundamentals of Machine learning	Understanding (1)
COL2	Study the Preparing to Model , Feature Engineering	Understanding (1) Applying (2)
COL3	Learn Modelling and Evaluation in Machine learning , privacy and threat models	Understanding (1)
COL4	Learn Malware Detection & Analysis	Understanding (1) Applying(2)
COL5	Learn Fraud Detection & Analysis	Understanding (1) Applying(2)

Mapping of CLOs with POs & PSOs

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	L	M	L	M			L				L	M	H	M	M
CLO2	H	M	H	L	M			M	L			M	M	H	H	M
CLO3	H	L	M	M	M			M	L	M		M	M	H	H	M
CLO4	H	H	H	M	H	H		M		H		M	H	M	M	M
CLO5	H	H	H	M	H	H		M		H		M	H	M	M	M

H: High, M: Medium, L: Low