CTMTAIDS SII P1: Advanced Machine Learning for Cyber Security and Forensics

Teaching Scheme					Evaluation Scheme									
L	T	P	C	TCH	Theory							Practical		Total
					Internal Exams					University Exams		University Exams (LPW)		
					TA-1		MSE		TA-2 *	Marks	Hrs	Marks	Hrs	
					Marks	Hrs	Marks	Hrs	Marks					
03	00	00	03	03	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives

1. To focus on recent advances in deep learning with neural networks.
2. To apply the concepts of machine learning for forensic investigation.
3. To understand a range of machine learning algorithms along with their strengths and weaknesses for computer forensics.
4. To understand and apply advanced machine learning algorithms to particular scenarios such phishing and spam filtering.
5. To identify machine learning methods to use and apply them rigorously in order to solve cyber security problems.

UNIT –I

Introduction to Machine Learning, Examples of Machine Learning applications Learning associations, Classification, Regression, Unsupervised Learning, Reinforcement Learning. Supervised learning- Input representation, Hypothesis class, Version space.

UNIT -II

Advanced machine learning topics: Bayesian modelling and Gaussian processes, randomized methods, Bayesian neural networks, approximate inference. Deep learning: regularization, convolutional neural networks, recurrent neural networks, variational autoencoders, generative models, applications.

UNIT -III

Applications of machine learning in natural language processing: recurrent neural networks, backpropagation through time, long short term memory, attention networks, memory networks, neural Turing machines, machine translation, question answering, speech recognition, syntactic and semantic parsing.

UNIT -IV

Introduction to Internet architecture, measuring Internet traffic behavior and anomaly detection, Live Demonstration: Analyze internet network traffic using unsupervised learning techniques, Applications of machine learning to network security, Supervised learning examples: Spam filtering, phishing, Unsupervised learning examples: Anomaly detection

UNIT -V

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.

Reference Books: -

1. Kevin P. Murphy. Machine Learning: A Probabilistic Perspective. MIT Press 2012
2. Ian Goodfellow, Yoshua Bengio and Aaron Courville. Deep Learning. MIT Press 2016
3. A Primer on neural networks for natural language processing, by Yaov Goldbeg.
4. R. G. Cowell, A. P. Dawid, S. L. Lauritzen and D. J. Spiegelhalter. "Probabilistic Networks and Expert Systems". Springer-Verlag. 1999.
5. M. I. Jordan (ed). "Learning in Graphical Models". MIT Press. 1998. Collection of papers. These appear collated here.
6. J. Pearl. "Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference." Morgan Kaufmann. 1988.
7. Graphical models by Lauritzen, Oxford science publications
8. F. V. Jensen. "Bayesian Networks and Decision Graphs". Springer. 2001.
9. Neural Networks and Deep Learning by Michael Nilson