GUJARAT TECHNOLOGICAL UNIVERSITY

Master of Engineering

WEF Academic Year	: 2021-22
Semester	: 2
Category of the Course	: Program Elective Course-III
Course Name & Code	: Artificial Intelligence in Cyber Security –II (4725904)

Prerequisite:

- Basics of artificial intelligent methods for preventing cyberspace

Rationale:

- The role of AI is important specifically in the current era where cyber security challenges are increasing. The subject will explore the migration of cyber challenges using Artificial Intelligence.

Course Scheme:

Teaching Scheme			Total Credits	Assessment Pattern and Marks				Total Marks
				Theory		Practical		
L	T	PR	C	ESE (E)	PA(M)	ESE (V)	PA (I)	
03	00	02	04	70	30	30	20	150

Course Content:

Sr No	Course Content	No of Hours	%
1	UNIT 1: Machine Learning and Cyber Security Cyber threat landscape, The cyber attacker's economy, A marketplace for hacking skills, Indirect monetization, The upshot, Adversaries using machine learning, Real-world uses of machine learning in security, Spam Fighting: An iterative approach, Limitations of machine learning in security, Machine Learning: problems and approaches, Machine Learning in practice: A worked example, overview of classification and clustering.	08	20
2	UNIT 2: Anomaly Detection using Artificially Intelligent Methods When to use anomaly detection versus supervised learning, Intrusion detection with heuristics, Data-driven methods, Feature engineering for anomaly detection, Host intrusion detection, Network intrusion detection, Web application intrusion detection, Anomaly detection with data and algorithms, Forecasting (supervised machine learning), Statistical metrics, Goodness-of-fit, Unsupervised machine learning algorithms, Density-based methods, Challenges of using machine	08	20

	learning in anomaly detection, Response and mitigation, Practical system design concerns, Optimizing for explainability, Maintainability of anomaly detection systems, Integrating human feedback, Mitigating adversarial effects.		
3	UNIT 3: Network Traffic Analysis using Artificially Intelligent Methods Theory of network defense, Access control and authentication, Intrusion detection, Detecting in-network attackers, Data-centric security, Honeypots, Machine learning and network security, From captures to features, Threats in the network, Botnets and you, Building a predictive model to classify network attacks, Exploring the data, Data preparation, classification, Supervised learning, Semi-supervised learning, Unsupervised learning, Advanced ensembling.	08	20
4	UNIT 4: Protecting the Consumer Web Monetizing the consumer web, Types of abuse and the data that can stop them, Authentication and account takeover, Account creation, Financial fraud, Bot activity, Supervised learning for abuse problems, Labeling data, Cold start versus warm start, False positives and false negatives, Multiple responses, Large attacks, Clustering abuse, Example: clustering spam domains, Generating clusters, Scoring clusters, Further directions in clustering.	06	20
5	UNIT 5: Adversarial Machine Learning Terminology, The importance of adversarial ML, Security vulnerabilities in machine learning algorithms, Attack transferability, Attack technique: model poisoning, Example: binary classifier poisoning attack, Attacker knowledge, Defense against poisoning attacks, Attack technique: evasion attack, Example: binary classifier evasion attack, Defense against evasion attacks.	06	15
6	UNIT 6: Recent Trends in AI for Cyber Security	04	05

Text Books/ Reference Books:

1. Machine Learning and Security by Clarence Chio and David Freeman, O'Reilly Media, Inc., ISBN: 9781491979907, February 2018.
2. AI in Cybersecurity by Leslie F. Sikos
   Springer International Publishing
3. Artificial Intelligence For Cyber Security Methods Issues And Possible Horizons Or Opportunities by Misra S.

Springer, 2021.

Course Outcome:

After completion of the Course, Students will be able to:

No	Course Outcomes	RBT Level*
01	Understand the machine learning-based approaches for cyber security applications.	UN
02	Usage artificial intelligence methods for anomaly detection.	AP
03	Examine the network traffic to build a predictive model for classifying network attacks.	AP
04	Compare & contrast classification and clustering methods for cyber security.	AN
05	Identify security vulnerabilities in machine learning algorithms.	AN

*RM: Remember, UN: Understand, AP: Apply, AN: Analyze, EL: Evaluate, CR: Create

Suggested Course Practical List:

- The practical work will be carried out based on the content covered during the academic sessions.

List of Laboratory/Learning Resources Required:

- Course-related online MOOCs on NPTEL/SWAYAM platform
- Recently Published papers/articles in reputed journals