GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Engineering

Level: Postgraduate

Branch: Computer Engineering (Cybersecurity)

Course / Subject Code: ME01059041

Course / Subject Name : Artificial Intelligence in Cyber Security-Part I

w. e. f. Academic Year:	2024-25
Semester:	I
Category of the Course:	Program Elective Course-01

Prerequisite:	• Fundamentals of Cyber Security and basics of Artificial Intelligence.
Rationale:	• Learners should be made aware of artificial intelligence-based methods for problem-solving. • They will also be able to understand different cybersecurity threats based on Artificial Intelligence-based techniques.

Course Outcome:

After Completion of the Course, Student will able to:

No	Course Outcomes	RBT Level
01	Understand the core concepts and practical aspects of artificial intelligence in the context of cyber security.	UN
02	Apply the artificial intelligence-based techniques for detecting cyber security threats.	AP
03	Apply the artificial intelligence-based methods for providing secure authentication mechanisms.	AP
04	Analyze the artificial intelligence-based detection and prevention approaches for cyber security.	AN
05	Evaluate the performance of artificial intelligence-based cyber security techniques.	EL

**Revised Bloom's Taxonomy (RBT)*

Teaching and Examination Scheme:

Teaching Scheme (in Hours)			Total Credits L+T+ (PR/2)	Assessment Pattern and Marks				Total Marks
				Theory		Tutorial / Practical		
L	T	PR	C	ESE (E)	PA / CA (M)	PA/CA (I)	ESE (V)	
3	0	2	4	70	30	20	30	150

GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Engineering

Level: Postgraduate

Branch: Computer Engineering (Cybersecurity)

Course / Subject Code: ME01059041

Course / Subject Name : Artificial Intelligence in Cyber Security-Part I

Course Content:

Unit No.	Content	No. of Hours	% of Weightage
1.	**Artificial Intelligence Core Concepts and Tools:** Evolution of AI: from expert systems to data mining, Types of machine learning, Algorithm training and optimization, AI in the context of cyber security, Setting up AI for cyber security arsenal, Python for AI and cyber security	8	20
2.	**Detecting Cyber Security Threats using AI**: Detecting spam with perceptron, Spam detection with SVMs, Phishing detection with logistic regression and decision trees, Spam detection with Naïve Bayes, Malware analysis at glance, Decision tree malware detectors, detecting metamorphic malware with HMMs, Advanced malware detection with deep learning, Network Anomaly detection techniques, Network attack classification, Detecting botnet topology, Different ML algorithms for botnet detection	10	30
3.	**Protecting Sensitive Information and Assets**: Authentication abuse prevention, account reputation scoring, User authentication with keystroke recognition, Biometric authentication with facial recognition, introducing fraud detection algorithm, Predictive analytics for credit card fraud detection, Evaluating the quality of predictions.	8	20
4.	**Evaluating and Testing AI Arsenal:** Best practices for featuring engineering, evaluating a detector's performance with ROC, using cross-validation for algorithms, Evading ML detectors, Challenging ML anomaly detection, Testing for data and model quality, Ensuring securing and reliability	8	20
5.	**Future Aspects:** Latest Developments in Artificial Intelligence for enhancement of Cyber Security for organizations.	6	10
	Total		**100**

Suggested Specification Table with Marks (Theory):

Distribution of Theory Marks (in %)					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
-	10	40	40	10	-

Where R: Remember; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (as per Revised Bloom's Taxonomy)

References/Suggested Learning Resources:

(a) Books:

1. Hands-On Artificial Intelligence for Cybersecurity by Alessandro Parisi Packt Publishing.
2. AI in Cybersecurity by Leslie F. Sikos Springer International Publishing.

(b) Open source software and website:

1. Scikit Learn (https://scikit-learn.org/stable/)
2. PyTorch (https://pytorch.org/)
3. TensorFlow (https://www.tensorflow.org/)
4. Weka (https://www.cs.waikato.ac.nz/ml/weka/)
5. Colab (https://colab.research.google.com/notebooks/welcome.ipynb)
6. Keras.io (https://keras.io/)
7. Pandas (https://pandas.pydata.org/)
8. Jupyter Notebook (https://jupyter.org/install)

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:

Suggested Project List:

Suggested Activities for Students: If any

Any Other:

* * * * * * *