WEF Academic Year	: 2021-22
Semester	: 1
Category of the Course	: Program Elective Course-I
Course Name & Code	: Artificial Intelligence in Cyber Security –I (4715904)

Prerequisite:

- Fundamentals of Cyber Security

Rationale:

- Learners should be made aware of artificial intelligence-based methods for problem-solving.
- They will also be able to understand different cybersecurity threats. Artificial Intelligence-based methods for detecting and preventing cybersecurity threats is the main objective of this course.

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: 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	6	25
2	Unit 2: Detecting Cyber Security Threats with 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	14	25
3	Unit 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	12	25
4	Unit 4: Evaluating and Testing AI Arsenal Best practising for featuring engineering, evaluating a detector's performance with ROC, using cross-validation for algorithms, Evading ML detectors, Challenging	10	25

	ML anomaly detection, Testing for data and model quality, Ensuring securing and reliability		

Reference Books:

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

Course Outcome:

After completion of the Course, Students will be 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 methods for detecting cyber security threats.	AP
03	Apply the artificial intelligence-based methods for providing secure authentication mechanisms.	AP
04	Analyse the artificial intelligence-based detection and prevention methods for cyber security.	AN
05	Evaluate the performance of artificial intelligence-based cyber security methods.	EL

*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:

- Windows and Linux latest release, IDE and Interpreter of Python.
- List of Open-Source Tools/Simulator:
    - Scikit Learn (https://scikit-learn.org/stable/)
    - PyTorch (https://pytorch.org/)
    - TensorFlow (https://www.tensorflow.org/)
    - Weka (https://www.cs.waikato.ac.nz/ml/weka/)
    - Colab (https://colab.research.google.com/notebooks/welcome.ipynb)
    - Keras.io (https://keras.io/)
    - Pandas (https://pandas.pydata.org/)
    - Jupyter Notebook (https://jupyter.org/install)
- List of Useful websites/MOOCs that are relevant to this course.