SARVAJANIK UNIVERSITY
Sarvajanik College of Engineering and Technology
Bachelor of Technology

Year: B. Tech III (Semester VI)

Subject Name: Artificial Intelligence for Cyber Security **Subject Code:** BTAI14602
Type of course: Professional Elective Course
Prerequisite: Search Algorithms in Artificial Intelligence

Rationale: Organizations today are spending billions of dollars globally on cybersecurity. Artificial Intelligence (AI) has emerged as a great solution for building smarter and safer security systems that allow you to predict and detect suspicious network activities, such as phishing or unauthorized intrusions, in your network. This Course presents and demonstrates the popular and successful AI approaches and models that you can adopt to detect potential attacks and protect your corporate systems.

Teaching and Examination Scheme:

Teaching Scheme				Theory Marks			Practical Marks		Total
L	T	P	C	TEE	CA1	CA2	TEP	CA3	
3	0	2	4	60	25	15	30	20	150

CA1: Continuous Assessment (assignments / projects / open book tests / closed book tests) CA2: Sincerity in attending classes / class tests / timely submissions of assignments / self-learning attitude / solving advanced problems TEE: Term End Examination TEP: Term End Practical Exam (Performance and viva on practical skills learned in course) CA3: Regular submission of Lab work / Quality of work submitted / Active participation in lab sessions / viva on practical skills learned in course.

Content:

Sr. No.	Contents	Total Hrs
1.	**Introduction to AI for Cybersecurity Professionals** Applying AI in cybersecurity, Evolution in AI: from expert systems to data mining, A brief introduction to expert systems Reflecting the indeterministic nature of reality, Going beyond statistics toward machine learning, Mining data for models, Types of machine learning: Supervised learning, Unsupervised learning, Reinforcement learning, Algorithm training and optimization: How to find useful sources of data, Quantity versus quality, Getting to know Python's libraries: Supervised learning example – linear regression, Unsupervised learning example – clustering, Simple NN example – perceptron, AI in the context of cybersecurity.	**10**
2.	**Setting Up AI for Cybersecurity Arsenal** Getting to know Python for AI and cybersecurity, Python libraries for cybersecurity,	**10**

	Anaconda – the data scientist's environment of choice, Playing with Jupyter Notebooks, Installing DL libraries.	
3.	**Detecting Cybersecurity Threats with AI** Detecting Email Cybersecurity Threats with AI, Phishing detection with logistic regression and decision trees, Spam detection with Naive Bayes, NLP to the rescue, Malware Threat Detection, Network Anomaly Detection with AI.	**10**
4.	**Protecting Sensitive Information and Assets** Securing User Authentication: Authentication abuse prevention, Account reputation scoring, User authentication with keystroke recognition,	**08**
5.	**Fraud Prevention with Cloud AI Solutions** Introducing fraud detection algorithms, Predictive analytics for credit card fraud detection, Getting to know IBM Watson Cloud solutions, Importing sample data and running Jupyter Notebook in the cloud	**07**

Suggested Specification table with Marks (Theory): (For B.Tech only)

Distribution of Theory Marks					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
20	25	10	05	00	00

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (Revised Bloom's Taxonomy)

Reference Books:

Sr. No	**Title of Book /Article**	**Author(s)**	**Publisher and details like ISBN**
1	Hands-On Artificial Intelligence for Cybersecurity	Alessandro Parisi	Packt Publishing Limited
2	Artificial Intelligence and Cybersecurity: Advances and Innovations	Ishaani Priyadarshini, Rohit Sharma	CRC Press
3	Artificial Intelligence, Cybersecurity and Cyber Defence	Daniel Ventre	WILEY

Note: Students should refer to the latest editions of books

Course Outcomes (CO):

Sr. No.	CO statements	Marks % weightage
CO-1	Explain key concepts and terminology of artificial intelligence in cyber security.	30%
CO-2	Setup and use various AI Tools for Cyber Security	15%
CO-3	Determine and detect the cyber security threats using Artificial Intelligence.	30%
CO-4	Explain the measures to protect sensitive information and assets and leverage the cloud solutions for fraud detection.	15%
CO-5	Utilize knowledge of this course to protect themselves and society against Cyber Attacks.	10%

List of Open learning website:

- https://www.ibm.com/in-en/security/artificial-intelligence
- https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity/

List of Open-Source Software:

- Python Libraries – Numpy, Anaconda
- Jupyter Notebook
- Deep Leaning Libraries

List of Experiments:

Sr. No	Practical Statements
1.	Getting to know Python for AI and cybersecurity:

Python libraries for AI, NumPy as an AI building block, NumPy multidimensional arrays, Matrix operations with NumPy, implementing a simple predictor with NumPy, Scikit-learn, Matplotlib and Seaborn, Pandas

2. Python libraries for cybersecurity:
   Pefile, Volatility, Installing Python libraries

3. Enter Anaconda – the data scientist's environment of choice:
   Anaconda Python advantages, Conda utility, installing packages in Anaconda, Creating custom environments, Some useful Conda commands

4. Playing with Jupyter Notebooks:
   Our first Jupyter Notebook, Exploring the Jupyter interface, What's in a cell? Useful keyboard shortcuts, Choose your notebook kernel

5. Installing DL libraries:
   Deep learning pros and cons for cybersecurity, TensorFlow, Keras, PyTorch, PyTorch versus TensorFlow

6. Detecting spam with Perceptrons

7. Phishing detection with logistic regression and decision trees

8. Malware Threat Detection

9. Network Anomaly Detection with AI