COURSE TITLE	**ARTIFICIAL INTELLIGENCE & CYBER SECURITY**
COURSE CODE	**01CC0607**
COURSE CREDITS	**3**

Objective:

1 This course explores the intersection of Artificial Intelligence (AI) and Machine Learning (ML) with the field of cybersecurity. Students will learn how AI/ML techniques are applied to address complex security challenges, including threat detection, vulnerability analysis, malware classification, and security automation. The course will cover key AI/ML algorithms relevant to security, the process of applying these techniques to security datasets, and the challenges and future directions of using AI in the cybersecurity domain, including adversarial AI and ethical considerations

Course Outcomes: After completion of this course, student will be able to:

1 Apply AI and machine learning algorithms to solve cybersecurity problems such as intrusion detection and anomaly detection.

2 Implement machine learning models using appropriate tools, techniques, and datasets for security applications.

3 Analyze the performance, strengths, and limitations of AI/ML models in real-world cybersecurity scenarios.

4 Evaluate different AI/ML approaches based on accuracy, efficiency, and suitability for cybersecurity challenges.

5 Design and develop intelligent cybersecurity solutions using AI/ML techniques to address emerging threats.

Pre-requisite of course: Solid understanding of fundamental Artificial Intelligence or Machine Learning concepts and algorithms. Proficiency in a programming language commonly used for AI/ML (e.g., Python) and relevant libraries (e.g., scikit-learn). Solid understanding of core cybersecurity concepts (e.g., network security, malware, vulnerabilities). Familiarity with data analysis and statistical concepts.

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
2	0	2	50	30	20	25	25

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Contents : Unit	Topics	Contact Hours
1	**Introduction to AI/ML in Cybersecurity** Overview of AI and Machine Learning Concepts: Supervised, Unsupervised, Reinforcement Learning (review focusing on relevance to security), Key ML Algorithms for Security: Classification (SVM, Decision Trees, Neural Networks), Clustering (K-Means, DBSCAN), Anomaly Detection (Isolation Forest, Autoencoders), The Role of Data in AI for Security: Types of security data (logs, network traffic, malware samples, threat feeds), data collection and preprocessing challenges, Cybersecurity Domains Benefiting from AI/ML: Network Security, Endpoint Security, Application Security, Threat Intelligence, Brief History and Evolution of AI in Cybersecurity	6
2	**AI/ML for Network Security** Intrusion Detection Systems (IDS) using AI/ML, Signature-based vs. Anomaly-based detection, Network Traffic Analysis using ML, Identifying malicious traffic, encrypted traffic analysis, Anomaly Detection in Network Behavior: Detecting unusual patterns indicative of attacks (e.g., port scanning, DDoS),, User and Entity Behavior Analytics (UEBA) Concepts, Applying ML to Network Flow Data	7
3	**AI/ML for Endpoint and Malware Security** Endpoint Detection and Response (EDR) with AI/ML: Detecting malicious processes, fileless malware,, Malware Analysis using ML: Static analysis (feature extraction from binaries),, Dynamic analysis (behavioral analysis), Malware Classification and Family Identification using ML,, Applying ML to System Call Traces and Process Monitoring, AI/ML for File Integrity Monitoring	6
4	**AI/ML in Threat Intelligence and Vulnerability Management** Automated Threat Intelligence Gathering and Analysis using AI/ML, Correlating and Prioritizing Threat Alerts, Applying ML to Natural Language Processing (NLP) for analyzing threat reports and security feeds, Vulnerability Prediction and Prioritization using ML, AI/ML for Phishing Detection and Spam Filtering, Identifying Malicious Domains and URLs	6
5	**Challenges, Adversarial AI, and Future Trends** Data Challenges in AI for Security: Lack of labeled data, data imbalance, concept drift, Adversarial Machine Learning in Cybersecurity, Understanding adversarial attacks on ML models (evasion, poisoning, model inversion), Defending Against Adversarial AI Attacks, Explainable AI (XAI) in Cybersecurity, The need for interpretability in security decisions, Ethical Considerations and Bias in AI for Security,, Emerging Trends: Reinforcement Learning in Security, Federated Learning for Threat Detection	7
Total Hours		**32**

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical 1** Setting up an AI/ML Environment for Security Tasks: Installing necessary libraries and tools (Python, scikit-learn, pandas, potentially a deep learning framework like TensorFlow or PyTorch).	2
2	**Practical 2** Exploring and Preprocessing a Cybersecurity Dataset: Loading and cleaning a dataset containing security-relevant information (e.g., network traffic logs or benign/malicious file features).	2
3	**Practical 3** Implementing a Simple Classification Model for Intrusion Detection: Training and testing a basic classification algorithm (e.g., Decision Tree or SVM) on a network intrusion dataset.	2
4	**Practical 4** Implementing an Anomaly Detection Model: Applying an unsupervised learning algorithm (e.g., Isolation Forest or K-Means) to detect anomalous patterns in a network or system behavior dataset.	2
5	**Practical 5** Feature Engineering for a Security Dataset: Extracting or creating relevant features from raw security data to improve model performance.	2
6	**Practical 6** Evaluating ML Model Performance using Security Metrics: Calculating and interpreting metrics like precision, recall, F1-score, and ROC curves for a security classification model.	2
7	**Practical 7** Applying ML for Basic Malware Classification: Using a dataset of malware features to train a model that can classify different malware families.	2
8	**Practical 8** Exploring a Tool Utilizing AI/ML for Security: Guided exploration or demonstration of a security tool (e.g., an open-source IDS with ML capabilities, a malware analysis platform) that incorporates AI/ML.	2
9	**Practical 9** Implementing a Simple Adversarial Attack: In a controlled environment, demonstrate a basic adversarial attack (e.g., slightly modifying a benign input to be classified as malicious by a trained model).	2
10	**Practical 10** Mini-Project: Applying AI/ML to a Cybersecurity Problem: Students choose a specific cybersecurity problem (e.g., phishing email detection, malicious URL identification) and apply an appropriate AI/ML technique, including data preparation, model selection, and evaluation.	2
Total Hours		**20**

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Textbook :

1 Darknet: Into the Digital Underworld, Eileen Ormsby, Znak Horyzont - Spoleczny Instytut Wydawniczy Znak, 2022

References:

1 The Web Application Hacker's Handbook, The Web Application Hacker's Handbook, Stuttard & Marcus Pinto, John Wiley, 2017

2 Practical Threat Intelligence and Data-Driven Analysis, Practical Threat Intelligence and Data-Driven Analysis, -Roberto Rodriguez & Jose Rodriguez, packt, 2021

Suggested Theory Distribution:

The suggested theory distribution as per Bloom's taxonomy is as follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery					
Remember / Knowledge	**Understand**	**Apply**	**Analyze**	**Evaluate**	**Higher order Thinking / Creative**
0.00	6.00	28.00	26.00	20.00	20.00

Instructional Method:

1 The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

2 The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.

3 Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory.

4 Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory.

Supplementary Resources:

1 NPTEL Course: "Foundations of Cyber Security" – IIT Kanpur

2 "Cyber Threat Intelligence" – University of Colorado Boulder (Coursera)

3 "Tor Mastery: The Definitive Dark Web Guide" (Udemy)

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)