AI in Cyber Security (v1: AI-First)

Course Code: DI05032041-aics

Course Information

Field	Details
Program	Diploma in Engineering
Branch	Information & Communication Technology
Level	Diploma
Semester	5
Academic Year	2026-2027
Category	Professional Elective - II
Prerequisites	Basic computer literacy (email, internet, mobile apps). No prior AI knowledge required.

Rationale

As Artificial Intelligence (AI) and Machine Learning (ML) continue to revolutionize digital landscapes, they present both unprecedented opportunities for defense and sophisticated new vectors for cyberattacks. This course, "AI in Cyber Security," is designed from an AI-first perspective to equip students with a fundamental understanding of how modern AI techniques can be leveraged to detect, prevent, and mitigate cyber threats. By blending core cybersecurity principles with cutting-edge AI/ML applications like Generative AI and Large Language Models (LLMs), this course ensures that ICT diploma students are prepared for the rapidly evolving threat landscape of the future. The difficulty is kept introductory, focusing on applied methodologies rather than deep mathematical foundations.

Course Outcomes

After completion of the course, students will be able to:

No.	Course Outcomes	RBT Level
CO1	Understand the intersection of AI and Cybersecurity, identifying the CIA triad in an AI context.	Understand
CO2	Apply AI-driven techniques to detect defensive threats like spam, phishing, and malware.	Apply
CO3	Analyze risks of AI-powered offensive attacks and adversarial machine learning vulnerabilities.	Analyze
CO4	Utilize Generative AI and LLMs for security operations including log analysis and report generation.	Apply
CO5	Evaluate ethical and governance considerations in the deployment of AI-based security solutions.	Evaluate

Teaching and Examination Scheme

Teaching Scheme (Hours)				Assessment Pattern (Marks)				
L	T	PR	C	Theory ESE	Theory CA	Practical CA	Practical ESE	Total
3	0	2	4	70	30	25	25	150

Course Content

Unit No.	Content	Hours	Weightage (%)
1	**Foundations of AI and Cybersecurity** 1.1 Introduction to Cyber Security: CIA Triad, Cyber Space, Threats, Vulnerabilities (Foundational Recap). 1.2 Evolution of Security: From static rule-based systems to dynamic AI-powered defense. 1.3 AI Fundamentals: Narrow vs. General AI, Machine Learning vs. Deep Learning (Conceptual overview). 1.4 Discriminative vs. Generative AI in security contexts. 1.5 The AI Security Lifecycle: Data collection, model training, and performance metrics.	9	22
2	**AI for Defensive Security** 2.1 Email & Communication Defense: ML models for spam and phishing detection. 2.2 AI in Malware Analysis: Anomaly detection vs. signature-based detection for malicious files. 2.3 Network Anomaly Detection: Identifying botnets and DDoS patterns using AI analytics. 2.4 AI-Based Authentication: Behavioral biometrics (keystroke dynamics) and adaptive user authentication.	9	22
3	**AI for Offensive Security & Adversarial ML** 3.1 AI-Powered Attacks: Automated reconnaissance and AI-generated social engineering (Deepfakes). 3.2 Adversarial Machine Learning: Understanding Evasion, Poisoning, and Model Inversion attacks. 3.3 Large Language Model (LLM) Risks: Prompt injection and data leakage vulnerabilities. 3.4 Modern Threat Landscape: How AI scales the speed and frequency of cyberattacks.	8	18
4	**Generative AI in Security Operations** 4.1 LLMs for Cyber Operations: Use of AI assistants (ChatGPT/Claude) in SOC environments. 4.2 Prompt Engineering for Security: Crafting effective prompts for log analysis and code auditing. 4.3 Automated Incident Response: Summarizing threat intelligence and generating incident reports. 4.4 AI in Vulnerability Management: Predictive analysis for prioritizing software patches.	8	19

Unit No.	Content	Hours	Weightage (%)
5	**Governance, Ethics and Future Trends** 5.1 AI Security Governance: Policies and best practices for implementing AI in organizations. 5.2 Ethical Considerations: Bias in models, fairness, and privacy transparency. 5.3 Regulatory Landscape: Overview of global and Indian AI security frameworks. 5.4 Future Directions: Autonomous security agents and Quantum-AI intersection.	8	19

Suggested Course Practical List

Sr. No	Practical Outcomes (PrOs)	Unit No.	Hrs.
1	**Email Classification:** Use a simple Python implementation (Scikit-learn) to classify emails as Spam or Ham.	2	2
2	**Network Anomaly Detection:** Analyze a set of network logs using statistical clustering (K-Means) to detect outliers.	2	2
3	**Biometric Authentication:** Implement a Python script to analyze keystroke timing as a biometric signature.	2	2
4	**Evasion Attack Simulation:** Modify input text to bypass the basic spam classifier built in PrO 1.	3	2
5	**Prompt Engineering for SOC:** Interact with an LLM to explain and deconstruct a malicious script snippet.	4	2
6	**Incident Report Automation:** Use an AI tool to generate a structured incident report from a raw server log.	4	2
7	**Phishing Feature Extraction:** Analyze a dataset of AI-generated phishing emails and identify features for detection.	3	4
8	**AI-Assisted Patching:** Use an LLM to identify vulnerabilities in a code snippet and generate a secure version.	4	4
9	**Deepfake Artifact Exploration:** Research and document artifacts that help in detecting Deepfake audio or video.	5	4
10	**Policy Generation:** Prompt an AI to generate a ”Responsible AI Use” policy for an organization.	5	2
11	**Ethical Case Study:** Research a real-world incident involving AI-based fraud and suggest mitigations.	5	4

Suggested Specification Table with Marks (Theory)

Unit	Unit Title	R	U	A	N	E	C	Total
Overall Distribution	Theory Marks Distribution	20	40	30	10	0	0	100

Legend: R: Remember; U: Understanding; A: Application; N: Analyze; E: Evaluate; C: Create

References/Suggested Learning Resources

Books

Sr. No.	Title of Book	Author	Publication
1	Hands-On Machine Learning for Cybersecurity	Soma Halder	Packt Publishing, 2018
2	AI for Cybersecurity	John Hopkins Specialization	Coursera/JHU, 2024
3	Cybersecurity Essentials	Charles J. Brooks et al.	Wiley, 2018
4	Adversarial Machine Learning	Anthony Joseph et al.	Cambridge Univ. Press, 2021

Open-source Software and Websites

1. Udemy: AI in Cyber Security - `https://www.udemy.com/course/ai-in-cyber-security/`
2. IITM Pravartak: AI-Powered Cybersecurity Mastery - `https://sl-courses.iitmpravartak.org.in/ai-cybersecurity-course-online`
3. Coursera: AI for Cybersecurity Specialization - `https://www.coursera.org/specializations/ai-for-cybersecurity`
4. OWASP AI Security Guide - `https://owasp.org/www-project-ai-security-guide/`
5. NIST Artificial Intelligence Resources - `https://www.nist.gov/artificial-intelligence`

Suggested Student Activities

1. **Phishing Analysis Challenge:** Groups analyze AI-generated vs. Human-generated phishing emails.
2. **Deepfake Awareness Workshop:** Students research tools used to create and detect deepfakes.
3. **Prompt Competition:** Designing the most effective security prompt for auditing a piece of code.
4. **Ethics Debate:** Discussions on the use of facial recognition and its privacy impact.

Laboratory/Learning Resources Required

Sr. No.	Laboratory/Learning Resources	Applicable To
1	**Computer System** Windows 10/11 or Linux with 8GB RAM, Python 3.9+ Environment.	All PrOs
2	**Software/Tools** VS Code/Jupyter, Scikit-learn, Access to LLM APIs (OpenAI/Claude/Local Llama).	PrOs 1-7