AI in Cyber Security (v3: Balanced)

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

The rapid convergence of Artificial Intelligence and Cybersecurity has created a new paradigm in digital protection and threat landscapes. This course, "AI in Cyber Security," offers a balanced curriculum that bridges the gap between traditional security foundations and modern AI-driven methodologies. Students will master core principles of cryptography, network security, and ethical hacking while simultaneously learning how AI automates defenses, identifies complex attack patterns, and assist in forensics investigation. This "perfect balance" ensures that ICT diploma students are grounded in time-tested security standards while being fully capable of utilizing cutting-edge AI tools to combat evolving cyber threats like Deepfakes and AI-powered malware.

Course Outcomes

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

No.	Course Outcomes	RBT Level
CO1	Explain foundational principles of cryptography and cybersecurity, identifying AI's role in modern data protection.	Understand
CO2	Implement defensive security measures for accounts and systems using both traditional and AI-based detection tools.	Apply
CO3	Analyze network traffic and offensive threats, including adversarial machine learning and AI-generated social engineering.	Analyze
CO4	Utilize Generative AI and LLMs for security operations, including auditing, log analysis, and automated reporting.	Apply
CO5	Perform digital forensics investigations and evaluate ethical/governance frameworks for AI in security.	Apply/Eval.

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 Cybersecurity & AI** 1.1 Overview of Security: CIA Triad, Security Architecture, and Common Terminology. 1.2 Cryptography Basics: Symmetric vs. Asymmetric ciphers, Public/Private keys, and Hashing. 1.3 AI Fundamentals: Narrow vs. General AI, Machine Learning vs. Deep Learning in security. 1.4 **AI Application:** How AI complements traditional ciphers and hashing for enhanced integrity.	8	18
2	**Defensive Security: Traditional & AI-Driven** 2.1 Access Control: Auth/Auth, Multi-factor auth, and AI-powered behavioral biometrics. 2.2 Malicious Software & Detection: Virus, Trojan, and AI-based anomaly detection for zero-day malware. 2.3 Network & Cloud Defense: Firewalls, VPNs, and AI-assisted network traffic monitoring. 2.4 **AI Application:** Moving from signature-based detection to dynamic AI-powered behavioral analysis.	8	18
3	**Offensive Security & Adversarial ML** 3.1 Ethical Hacking Fundamentals: Steps of hacking (5-step process) and Kali Linux toolsets. 3.2 Adversarial Machine Learning: Evasion, Poisoning, and Model Inversion attacks explained. 3.3 AI-Generated Threats: Automated reconnaissance, AI-phishing, and Deepfake generation. 3.4 **AI Application:** Utilizing AI to identify vulnerabilities and simulating AI-powered social engineering attacks.	8	18
4	**Security Operations & Generative AI** 4.1 SOC Operations: Incident response, Log analysis, and Threat Intelligence. 4.2 Generative AI in Security: Using LLMs for code auditing, script explanation, and security reporting. 4.3 Vulnerability Management: AI-assisted patching and predictive vulnerability scanning. 4.4 **AI Application:** Collaborative security: Humans and AI assistants working in SOC environments.	9	22

Unit No.	Content	Hours	Weightage (%)
5	**Forensics, Ethics & Future Trends** 5.1 Digital Forensics: Forensic process, Artifact collection, and Tools (Autopsy/FTK). 5.2 Governance & Ethics: Bias in AI models, Privacy transparency, and Global/Indian AI frameworks. 5.3 Emerging Trends: Autonomous security agents and the intersection of Quantum and AI. 5.4 **AI Application:** AI-driven forensic analysis and detecting Deepfake evidence in digital investigations.	9	24

Suggested Course Practical List

Sr. No	Practical Outcomes (PrOs)	Unit No.	Hrs.
1	Implement Symmetric & Asymmetric Cryptography algorithms in Python.	1	2
2	Implement MD5 and SHA hashing for data integrity verification (Python).	1	2
3	**ML Classification:** Use Scikit-learn to classify emails as Spam or Ham.	2	2
4	Perform brute-force simulation and use an AI assistant to analyze the resulting security logs.	2	2
5	Use Nmap for network scanning and prompt an LLM to explain the port scanning results.	3	2
6	Perform packet sniffing (Wireshark) and use AI to identify anomalous traffic patterns.	3	2
7	Perform vulnerability scanning using Kali Linux and generate an AI-assisted remediation report.	4	2
8	**Code Auditing:** Use an LLM to identify vulnerabilities in a C/JS snippet and generate a secure version.	4	4
9	Perform forensic analysis on a provided disk image using Autopsy or FTK Imager.	5	4
10	**Deepfake Research:** Research and document a case of Deepfake fraud and list detection artifacts using AI tools.	5	4
11	**Policy Drafting:** Prompt an AI to generate a "Responsible AI Use" policy for a small business.	5	2

Suggested Specification Table with Marks (Theory)

Unit	Unit Title	R	U	A	N	E	C	Total
Overall Distribution	Theory Marks Distribution	25	40	25	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	Cryptography & Network Security	William Stallings	Pearson, 2019
2	Hands-On Machine Learning for Cybersecurity	Soma Halder	Packt Publishing, 2018
3	Ethical Hacking	Daniel Graham	No Starch Press, 2021
4	AI for Cybersecurity	John Hopkins Specialization	Coursera/JHU, 2024

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. **CTF Challenge:** Participate in an AI-focused Capture The Flag (CTF) competition.
2. **AI Tool Review:** Comparative study of traditional vs. AI-powered security products.
3. **Deepfake Seminar:** Presenting detection techniques for Generative AI media.
4. **Ethical Debate:** Discussing the implications of AI in surveillance vs. privacy.

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, Kali Linux, Wireshark, Nmap, Autopsy, FTK Imager, Access to LLMs.	PrOs 1-11