AI in Cyber Security (v2: Minimal AI)

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

In an era of pervasive digital connectivity, Cyber Security remains a vital shield against evolving threats. This course, "AI in Cyber Security," provides a foundational introduction to Cyber Space and its associated threats (malware, phishing, hacking), ensuring students from all backgrounds - including those who have not taken a dedicated security subject - can grasp essential security concepts. It covers core principles like the CIA triad, passwords, MFA, firewalls, and cyber laws (IT Act) alongside contemporary AI and Machine Learning (ML) techniques. While mastering traditional security principles and tools remains essential, students will also explore how AI can automate threat detection, improve malware analysis, and strengthen digital forensics. Simultaneously, the course addresses the emerging risks of AI-powered attacks and vulnerabilities in AI systems themselves. This hybrid approach ensures that ICT diploma students are equipped with both time-tested defensive strategies and the cutting-edge AI-assisted tools necessary for the modern security landscape.

Course Outcomes

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

No.	Course Outcomes	RBT Level
CO1	Understand fundamental principles of cyber space, cyber threats, CIA triad, and cryptography, including AI's impact on data protection.	Understand
CO2	Implement security strategies for authentication, authorization, and defense against malicious software, incorporating AI-based detection.	Apply
CO3	Apply secure protocols for web, network, and system protection, utilizing AI for anomaly monitoring.	Apply
CO4	Conduct ethical hacking using Kali Linux tools, enhanced by AI-assisted vulnerability discovery.	Apply

No.	Course Outcomes	RBT Level
CO5	Analyze cybercrimes and forensic evidence, addressing AI-driven threats like Deepfakes.	Analyze

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	**Cyber Space, Threats & Cryptography Fundamentals** 1.1 Cyber Space and Cyber Security Foundation: Definition, CIA triad, and OSI Security Architecture. 1.2 Cyber Threats & Terminology: Overview of Cyber Threats (Internal vs External), Adversary, Attack, Risk, Asset, Vulnerability. 1.3 Private & Public Key Cryptography: Principles and use cases. 1.4 Hashing Algorithms: MD5 and SHA for data integrity. 1.5 **AI Application:** Role of AI in modern protection; how AI enhances and challenges traditional cryptography.	8	18
2	**Account, Data & AI-Enhanced Security** 2.1 Authentication & Authorization: Password hygiene, Biometrics, Multi-factor auth (MFA), SSO, and CAPTCHA. 2.2 Malicious Software: Virus, Worm, Trojan Horse, Keylogger, Sniffer, Backdoor, Ransomware. 2.3 Defensive Measures: Firewalls (Packet filter, Application proxy), Antivirus concepts, Cloud security basics. 2.4 Account Attacks: Brute force, Social Engineering, Phishing (Vishing, Smishing), Machine-in-the-middle. 2.5 **AI Application:** AI in behavioral biometrics and AI-driven malware detection systems.	8	18

Unit No.	Content	Hours	Weightage (%)
3	**Network, System & AI-Powered Monitoring** 3.1 Web Security threats: Integrity, Confidentiality, Denial of service. 3.2 Network Ports & Protocols: Importance of ports, SSL/TLS, HTTPS, SSH, WAP security. 3.3 VPN (Virtual Private Networks): Secure remote access. 3.4 **AI Application:** AI for network traffic analysis, identifying botnets, and DDoS pattern recognition.	8	18
4	**Ethical Hacking & AI-Assisted Penetration Testing** 4.1 Basics of Ethical Hacking: Types of Hackers, Hacking terminology (Vulnerability, Exploit, 0-Day). 4.2 Five Steps of Hacking: Info Gathering, Scanning, Gaining/Maintaining Access, Covering Tracks. 4.3 Introduction to Kali Linux: Footprinting, Port Scanning, Password Cracking, Injection attacks. 4.4 **AI Application:** Using LLMs (ChatGPT/Claude) for script auditing, vulnerability explanation, and security reporting.	9	22
5	**Cyber Laws, Forensic & AI-Based Investigation** 5.1 Introduction to Cyber Crime: Types and classifications, Indian IT Act, Cyber Laws, and Digital Privacy. 5.2 Cyber Forensics: Overview, Disk, Network, Mobile, and Email Forensics. 5.3 Digital Forensics Tools: Autopsy, FTK Imager. 5.4 Basic Cyber Awareness & Practices: Password management, safe browsing, data privacy, incident reporting. 5.5 **AI Application:** AI-driven crimes (Deepfakes, AI-powered Phishing) and the use of AI in cyber forensic analysis.	9	24

Suggested Course Practical List

Sr. No	Practical Outcomes (PrOs)	Unit No.	Hrs.
1	Implement Substitution (Caesar Cipher) & Column Transformation in Python.	1	2
2	Implement Private key Cryptography algorithm in Python.	1	2
3	Implement MD5 and SHA hashing using Python.	1	2
4	Simulate a brute-force attack to crack passwords and measure strengths (Python/Tool).	2	2
5	**AI Application:** Use an AI assistant to analyze security logs and detect a failed login pattern.	2	2

Sr. No	Practical Outcomes (PrOs)	Unit No.	Hrs.
6	Set up Multi-Factor Authentication (MFA) and configure Antivirus/Firewall rules for protection.	2	2
7	Use Nmap to scan a network and identify open ports on a system.	3	2
8	Perform packet sniffing and password analysis using Wireshark.	3	2
9	**AI Application:** Use an AI-powered tool or LLM to explain the traffic patterns observed in Wireshark.	3	2
10	Basic Kali Linux commands and configuration in a virtual environment.	4	2
11	Perform vulnerability scanning using Kali Linux tools.	4	2
12	**AI Application:** Prompt an LLM to generate a secure version of a piece of vulnerable code.	4	2
13	Perform forensic analysis (Registry/Artifacts) using FTK Imager or Autopsy.	5	2
14	**Cyber Awareness:** Conduct/Prepare a cyber hygiene checklist or seminar on deepfake detection.	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	Computer Security: Principles and Practice	William Stallings	Pearson, 2017
3	Hands-On Machine Learning for Cybersecurity	Soma Halder	Packt Publishing, 2018
4	Ethical Hacking	Daniel Graham	No Starch 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. **Case Study Analysis:** Identify vulnerabilities in a real-world cyber attack.
2. **Hack-a-thon:** Participate in Capture The Flag (CTF) events.
3. **AI Tools Review:** Compare traditional Nmap scans with AI-assisted report generation.
4. **Cyber Awareness:** Conduct a seminar on deepfake detection.

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 1-14