GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Diploma in Engineering

Level: Diploma

Branch: Information & Communication Technology

Course / Subject Code: PEC-04/03

Course / Subject Name: AI in Cyber Security

w. e. f. Academic Year:	2026-27
Semester:	5
Category of the Course:	Professional Elective - II

Prerequisite:	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 Outcome:

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

No	Course Outcomes	RBT Level
01	Understand fundamental principles of cyber space, cyber threats, CIA triad, and cryptography, including AI's impact on data protection.	R, U
02	Implement security strategies for authentication, authorization, and defense against malicious software, incorporating AI-based detection.	U, A
03	Apply secure protocols for web, network, and system protection, utilizing AI for anomaly monitoring.	R, U, A
04	Conduct ethical hacking using Kali Linux tools, enhanced by AI-assisted vulnerability discovery.	R, U, A
05	Analyze cybercrimes and forensic evidence, addressing AI-driven threats like Deepfakes.	R, U, A

**Revised Bloom's Taxonomy (RBT)*

Teaching and Examination Scheme:

Teaching Scheme (in Hours)			Total Credits L+T+ (PR/2)	Assessment Pattern and Marks				Total Marks
				Theory		Tutorial / Practical		
L	T	PR	C	ESE (E)	PA / CA (M)	PA/CA (I)	ESE (V)	
3	0	2	4	70	30	25	25	150

Course Content:

Unit No.	Content	No. of Hours	% of Weightage
1.	**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.	08	18
2.	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.	08	18
3.	**3. Network, System & AI-Powered Monitoring** 3.1. Web Security threats: Integrity, Confidentiality, Denial of service.	08	18

	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.		
4	**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.	09	22
5.	**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.	09	24
	Total	**45**	**100**

Suggested Specification Table with Marks (Theory):

Distribution of Theory Marks (in %)					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
20	30	50	--	--	--

Where R: Remember; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (as per Revised Bloom's Taxonomy)

References/Suggested Learning Resources:

(a) Books:

1. Cryptography and Network Security by William Stallings, Pearson Education, 7th Edition, 2017, ISBN: 9789332585493

2. Computer Security: Principles and Practice by William Stallings and Lawrie Brown, Pearson Education, 3rd Edition, 2015, ISBN: 9789332575777
3. Hands-On Machine Learning for Cybersecurity by Soma Halder and Sinan Ozdemir, Packt Publishing, 1st Edition, 2018, ISBN: 9781788992282
4. The Web Application Hacker's Handbook by Dafydd Stuttard and Marcus Pinto, Wiley, 2nd Edition, 2011, ISBN: 9781118026472
5. Ethical Hacking and Penetration Testing Guide by Rafay Baloch, Auerbach Publications, 1st Edition, 2014, ISBN: 9781482231618
6. Machine Learning and Security by Clarence Chio and David Freeman, O'Reilly Media, 1st Edition, 2018, ISBN: 9781491979907

(b) Open-source software and website:

- Software
  - Kali Linux
  - Wireshark
  - Nmap
  - Metasploit Framework
  - Autopsy (Digital Forensics)
  - FTK Imager
- Online Tutorials
  - OWASP AI Security Guide
  - NIST Artificial Intelligence Resources
- Comprehensive Courses
  - GIAN: Explainable AI for Cybersecurity
  - Cyber Security and Privacy By Prof. Saji K Mathew, IIT Madras
  - Udemy: AI in Cyber Security
  - IITM Pravartak: AI-Powered Cybersecurity Mastery
  - Coursera: AI for Cybersecurity Specialization
  - AI & Cybersecurity by Jeff Crume
  - Machine Learning for Cyber Security
  - Masterclass - Agentic AI for Security Professionals
  - Cyber Security Training for Beginners

Suggested Course Practical List

Sr. No.	Practical Outcomes (PrOs)	Unit No.	Approx. Hrs. required
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
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
	Total		**30**

List of Laboratory/Learning Resources Required:

Sr. No.	Equipment Name with Broad Specifications	PrO. No.
1	Computer with latest configuration (minimum 8GB RAM, i5 processor) with Windows/Linux/Mac Operating System	All
2	**Software/Tools:** VS Code/Jupyter, Kali Linux, Wireshark, Nmap, Autopsy, FTK Imager, Access to LLMs.	All

Suggested Project List:

A suggestive list of micro-projects is given here. Similar micro-projects could be added by the concerned course teacher:

1. **AI-Based Phishing Detection System:** Detect phishing URLs/emails using ML models or rule-based + AI approach.

2. **Network Intrusion Detection System (NIDS):** Monitor network traffic and detect anomalies using AI techniques.
3. **Password Strength Analyzer with AI Suggestions:** Evaluate password strength and suggest improvements using AI.
4. **Log Analyzer using AI/LLM:** Analyze system/server logs and detect suspicious login patterns.
5. **Ransomware Behavior Simulation & Detection:** Simulate ransomware behavior and build a detection mechanism.
6. **AI Chatbot for Cyber Awareness:** Chatbot that educates users about cyber threats and safe practices.
7. **Deepfake Detection Prototype:** Basic system to detect manipulated images/videos using available tools/APIs.
8. **Secure File Transfer System with Encryption:** Implement encryption + authentication for secure communication.
9. **Web Vulnerability Scanner (Basic):** Detect SQL injection, XSS vulnerabilities (basic level).
10. **Cyber Incident Reporting Portal:** Platform to report and categorize cyber incidents with basic analytics.

Suggested Activities for Students:

1. **Cyber Attack Case Study Analysis:** Analyze real-world cyber incidents (e.g., ransomware, phishing attacks) and identify vulnerabilities, attack vectors, and preventive strategies.
2. **Capture The Flag (CTF) Participation:** Engage students in ethical hacking challenges to develop practical skills in reconnaissance, exploitation, and defense.
3. **AI Tools in Cybersecurity Review:** Compare traditional tools (e.g., Nmap, Wireshark) with AI-assisted tools for threat detection and reporting.
4. **Cyber Awareness Campaign:** Design and conduct awareness sessions on topics like phishing, password hygiene, and deepfake detection.
5. **Hands-on Security Lab Workshops:** Perform activities like port scanning, packet analysis, and vulnerability assessment using Kali Linux tools.
6. **AI-Based Threat Detection Demo:** Use simple ML/AI tools or LLMs to analyze logs and identify suspicious patterns.
7. **Group Discussion on Cyber Laws:** Discuss provisions of the IT Act, digital privacy, and recent cybercrime cases in India.
8. **Mini Seminar on Emerging Threats:** Topics like AI-powered attacks, deepfakes, ransomware evolution, etc.
9. **Secure Coding & Debugging Practice:** Identify vulnerabilities in sample code and improve it using AI assistance.

* * * * * * *