

PRASAD V. POTLURI SIDDHARTHA INSTITUTE OF TECHNOLOGY

(Autonomous)

Kanuru, Vijayawada-520007

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (AI&ML)

IV B.Tech I Semester

Cyber Security

Course Code	20AM4703B	Year	IV	Semester	I
Course Category	PEC	Branch	CSE (AI&ML)	Course Type	Theory
Credits	3	L-T-P	3-0-0	Prerequisites	Cryptography and Network Security
Continuous Internal Evaluation	30	Semester End Evaluation	70	Total Marks	100

Course Outcomes

Upon Successful completion of course, the student will be able to

CO1	Describe cybersecurity concepts, threats, attacks, and defenses to understand governance challenges and the role of security policies.	L2
CO2	Apply cyber offense planning, attack vectors, and tools to identify and demonstrate common cybercrime techniques.	L3
CO3	Apply tools and techniques to analyze cybercrimes involving mobile devices, wireless networks, and identity-based threats.	L3
CO4	Analyze AI-based detection strategies to improve malware and network anomaly identification.	L4

Contribution of course outcomes towards achievement of program outcomes & Strength of correlations (3: Substantial,2: Moderate,1: Slight)

[illegible]

PRASAD V. POTLURI SIDDHARTHA INSTITUTE OF TECHNOLOGY

(Autonomous)

Kanuru, Vijayawada-520007

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (AI&ML)**IV B.Tech I Semester**

Syllabus		
Unit No	Contents	Map ped CO
I	Introduction to Cyber Security: Basic Cyber Security Concepts, layers of security, Vulnerability, threat, Harmful acts, Internet Governance – Challenges and Constraints, Computer Criminals, CIA Triad, Assets and Threat, motive of attackers, active attacks, passive attacks, Software attacks, hardware attacks, Spectrum of attacks, Taxonomy of various attacks.	CO1
II	Cyber Offenses: Criminals Planning Them: Introduction, planning of Attacks, Social Engineering, Cyber stalking, Cyber Cafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector, Cloud Computing.	CO1, CO2
III	Cybercrime: Mobile and Wireless Devices: Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication service Security, Attacks on Mobile/Cell Phones, Organisational Measures for handling mobile, Organizational security Policies and Measures in Mobile Computing Era, Laptops.	CO1, CO3, CO4
IV	Tools and Methods Used in Cybercrime: Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Keyloggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow.	CO1, CO3, CO4
V	Malware Threat Detection: Artificial intelligence for malware detection: Malware goes by many names, Malware analysis tools of the trade, Malware detection strategies Static malware analysis, Static analysis methodology. Network Anomaly Detection with AI: Network anomaly detection techniques, Anomaly detection rationales, Intrusion Detection Systems, Host Intrusion Detection Systems, Network Intrusion Detection Systems, Anomaly-driven IDS.	CO1, CO3, CO4

Learning Resources	
Text Books	
1. Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Sunit Belapure and Nina Godbole, First Edition, 2013, Wiley India. 2. Hands-On Artificial Intelligence for Cybersecurity, Alessandro Parisi, First Edition, August 2019, O'Reilly.	
References	
3. Cyber Law simplified, Vivek Sood, Eleventh Edition, 2013, Mc-Graw Hill. 4. Cyber security and Cyber Laws, Alfred Basta, Nadine Basta, Mary brown, Ravindra Kumar, First Edition, 2018, Cengage Learning.	
E-Recourses and other Digital Material	
1. https://www.cybo k.org/media/downloads/CyBOK- version-1.0.pdf 2. https://onlinecourses.nptel.ac.in /noc23_cs127/preview 3. https://onlinecourses.swayam2.ac.in/nou19_cs08/preview 4. https://onlinecourses.swayam2.ac.in/cec20_cs15/preview 5. https://www.coursera.org/learn /cybersecurity-for-everyone	