TEERTHANKER MAHAVEER UNIVERSITY

(Established under Govt. of U. P. Act No. 30, 2008)

Delhi Road, Moradabad (U.P.)

PhD PROGRAMME

SYLLABUS FOR DISCIPLINE-SPECIFIC COURSE
COMPUTER APPLICATIONS/
COMPUTER SCIENCE & ENGINEERING

Course Code: PDS240136	**CYBER SECURITY AND PRIVACY**	**L**	**T**	**P**	**C**
		0	**0**	**0**	**4**
Objective:	To gain knowledge of cryptographic principles, algorithms, and protocols for securing data and ensuring confidentiality. To explore advanced authentication techniques, network security mechanisms and privacy principles, data protection techniques, and threat detection and critical infrastructure security.				
Course Outcomes:					
CO 1:	understanding of cryptographic principles and techniques, including symmetric and asymmetric encryption, hashing algorithms, digital signatures, and advanced protocols, to ensure data confidentiality, integrity, and authenticity in cybersecurity contexts.				
CO 2:	Design and implement robust identity verification systems by applying diverse authentication methods, including multi-factor and biometric techniques, while addressing challenges associated with decentralized identity and zero-trust authentication frameworks.				
CO 3:	Evaluate network security mechanisms, including firewalls, IDS/IPS, VPNs, and secure architectures, to mitigate threats such as spoofing, DDoS, and man-in-the-middle attacks, while ensuring the security of IoT and cloud networks.				
CO 4:	Evaluate privacy principles and data protection techniques, including differential privacy, k-anonymity, and IAM systems, to address privacy challenges, and compliance with regulatory frameworks				
CO 5:	Explore advanced cybersecurity applications in critical infrastructure, including emerging research trends like post-quantum cryptography, AI-driven threat detection, and cyber-physical systems security, leveraging real-world case studies to develop effective mitigation strategies.				
Course Content:					
Unit 1:	Overview of cryptography and its role in cybersecurity. Symmetric encryption: algorithms, applications, and limitations. Asymmetric encryption: principles, RSA, ECC, and key management. Hashing techniques: MD5, SHA family, and their applications. Digital signatures and certificates: ensuring authenticity and integrity. Advanced cryptographic techniques: quantum cryptography and homomorphic encryption. Cryptographic protocols: SSL/TLS, and IPsec.				
Unit 2:	Overview of authentication and its role in security. Authentication methods: knowledge-based (passwords, PINs), possession-based (tokens, OTPs), and inherence-based (biometrics). Multi-factor authentication (MFA) and adaptive authentication techniques. Password management and best practices. Biometric authentication: fingerprint, facial recognition, and behavioral biometrics. Challenges and emerging trends: decentralized identity, zero-trust authentication, and password less systems.				

Unit 3:	Firewalls, intrusion detection/prevention systems (IDS/IPS), and VPNs. Network attacks: spoofing, man-in-the-middle, and DDoS. Wireless network security and IoT device protection. Secure network architectures, Cloud network security challenges and solutions
Unit 4:	Privacy principles: anonymity, pseudonymity, and differential privacy. Techniques for privacy-preserving computation: k-anonymity and secure multi-party computation. Data protection frameworks: GDPR, HIPAA, and data masking techniques. Identity and access management (IAM) systems and zero-trust architecture. Privacy challenges in AI and big data environments.
Unit 5:	Security in critical infrastructure, including power grids, healthcare, and financial systems. AI for threat detection, adversarial machine learning, and autonomous security systems. Big data analytics for threat intelligence and anomaly detection. Post-quantum cryptography, cyber-physical systems security, and ethical concerns in cybersecurity research. Real-world case studies on cybersecurity breaches and mitigation strategies.
Text Books:	1. Bruce Schneier, "Applied Cryptography". John Wiley & Sons 2. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson Education.
Reference Books:	1. Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill Education. 2. Charles P. Pfleeger and Shari Lawrence Pfleeger, Security in Computing, Prentice Hall. 3. Michael T. Goodrich and Roberto Tamassia, Introduction to Computer Security, Pearson Education.