NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	Integrated BTech (CSE)-MBA
Course Code:	3CS213ME24
Course Title:	Data Privacy
Course Type:	Department Elective-VI
Year of Introduction:	2024-25

L	T	Practical Component				C
		LPW	PW	W	S	
3	0	2	-	-	-	4

Course Learning Outcomes (CLO):

At the end of the course, the students will be able to –

1. summarise the concepts of web security and privacy, hardware and software vulnerabilities, and protection mechanisms (BL2)
2. identify the need for data privacy and the related technologies (BL3)
3. analyse the requirements of attacks and secure data-sharing practices with privacy preservation policies (BL4)
4. design the protection mechanisms against several data-related attacks. (BL6)

Unit	Contents	Teaching Hours (Total 45)
Unit-I	**Introduction to Security:** Cryptography Basics, Web security considerations, Protocols- SSL/TLS, SET, Secure Shell, Hardware vulnerabilities- Backdoor, Hardware Trojans, Software vulnerabilities: Buffer Overflow, XSS, SQL injection, Prevention and Counter Measures, Threat Modelling	07
Unit-II	**Privacy Preservation Schemes:** Data localization issues, Managing personally identifiable or sensitive information, Hippocratic databases, Homomorphic Encryption, Identity-Based Encryption, Differential privacy, Privacy-preserving data analysis	12
Unit-III	**Disclosure Control:** Introduction, Data Quality vs. Anonymity, Data linkage, Disclosure Control Techniques, Data Anonymization, Models of Protection- null map, k-map, wrong-map	10
Unit-IV	**Data Explosion**: Availability vs. Storage vs. Collection Trade-off, Barriers to distribution, Mathematical models for sharing practices and policies for computing privacy and risk measurements	08
Unit-V	**Mechanisms of Backup and Disaster Recovery Tools:** Backup Mechanisms- Restor points, Failover, Failback, Data Replication, Disaster recovery tools: Carbonite, Arcserve, Veritas, Recent Data Privacy Use Cases: Healthcare, Internet of Vehicles.	08

Self-Study:

The self-study contents will be declared at the commencement of the semester. Around 10% of the questions will be asked from self-study contents

Suggested Readings/ References:

1. Stallings, W. Cryptography and Network Security. Pearson Education.
2. Giannotti, F., & Pedreschi, D. (Eds.). Mobility, data mining, and privacy: Geographic knowledge discovery. Springer Science & Business Media.
3. Bygrave, L. A. Data privacy law: an international perspective, Oxford: Oxford University Press.
4. Scoble, R., Israel, S., & Benioff, M. R. Age of context: Mobile, sensors, data and the future of privacy. USA: Patrick Brewster Press.
5. Katharine Jarmul, Practical Data Privacy: Enhancing Privacy and Security in Data, O'Reilly

Suggested List of Experiments:

Sr. No.	Title	Hours
1	Installation and Study of Openssl- Implementation of Encryption/Decryption algorithms, Hashing, and Digital Signature generation in OpenSSL	04
2	Certificate authority creation and installation using Openssl.	02
3	Generation of password wordlist using CRUNCH and analyse using JOHN-THE-RIPPER.	02
4	Threat modeling using Microsoft Threat Modeling Tool	04
5	Installation of Kali Linux using VMware and installation of toolkits for phishing and DoS attacks	04
6	Study of stack and buffer overflow attacks.	02
7	Analyze SYN flooding attacks through Low orbit ION Cannon tool	02
8	Implement SQL injection attack on a target system	02
9	Develop secure coding practices to handle Code Injection Vulnerabilities such as SQL Injection, PHP Injection, and Command Injection	04
10	Installation of SNORT intrusion detection system and analyse of the malicious network traffic	04