20CS008 CYBER SECURITY & LAWS

Hours Per Week :

L	T	P	C
3	-	-	3

Total Hours :

L	T	P
45	-	-

WA/RA	SSH/HSH	CS	SA	S	BS
15	30	-	5	5	-

Course Description and Objectives:

To understand the basics of cyber law, crimes, its related issues and ethical laws of computer.

Course Outcomes:

Upon completion of this course, student should able to :

- ✓ Explain blockchain technology and its immutable property
- ✓ Know the working of distributed ledger
- ✓ Analyse the different consensus protocols
- ✓ Use Ethereum to implement Blockchain
- ✓ Apply blockchain techniques in different applications

SKILLS:

- ✓ Understand about various case studies and analyze the reasons that led to cyber crimes
- ✓ Forensics investigation
- ✓ Precautions to overcome online scams

UNIT – I

Introduction to cyber crime and cyber offences:
Introduction- Cyber crime definitions – Cyber crime and Information Security- Cyber Criminals-Classification of Cybercrimes-An Indian Perspective- How criminals plan attacks- Social Engineering- Cyber Stalking- Cyber cafe and Cyber crimes- Botnets- Attack Vectors- Cloud Computing

UNIT - II

Cybercrime: Mobile and Wireless Devices:

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, Mobile Devices: Security Implications for Organizations, Organizational Measures for Handling Mobile, Devices-Related Security Issues, Organizational Security Policies and Measures in Mobile Computing Era, Laptops

UNIT - III

Tools and methods used in cyber crime

Proxy servers and Anonymizers- Phishing Password crackingKey loggers and Spy wares-Virus and worms-Trojan Horse and Backdoors-Steganography-SQL Injection-Buffer overflow-Attacks on wireless network. Phishing and Identity Theft

UNIT - IV

Understanding computer forensic:
Historical background of cyber forensic-Forensic analysis of e-mail-Digital forensic life cycle-Network forensic-Setting up a computer forensic Laboratory-Relevance of the OSI 7 Layer model to computer Forensic-Computer forensics expertise in India- Challenges in Computer forensics

UNIT - V

Introduction to the Legal Perspectives of Cybercrimes and Cyber security: Cybercrime and the Legal Landscape around the World, Why Do We Need Cyber laws, The Indian IT Act, Challenges to Indian Law and Cybercrime Scenario in India, Consequences of Not Addressing the Weakness in Information Technology Act, Digital Signatures and the Indian IT Act, Cybercrime and Punishment

TEXTBOOKS:

1. Nina Godbole & Sunit Belapure “Cyber Security”, Wiley India, 2011.

REFERENCEBOOKS:

1. Mark F Grady, Fransesco Parisi, “The Law and Economics of Cyber Security”, Cambridge University Press, 2006
2. Jonathan Rosenoer, “Cyber Law: The law of the Internet”, Springer-Verlag, 1997.
3. Sudhir Naib, The Information Technology Act, 2005: A Handbook, OUP, New York, (2011)
4. Jon Friedman. Mark Bouchard, CISSP. Foreword by John P. Watters, Cyber Threat Intelligence, Definitive Guide TM, 2015.