School of Engineering
B. Tech. (CSE) with Specialization Cyber Security
(In Association with EC-Council)

Semester – II

BCO 173A	**Certified Secure Computer User**	**4-0-0 [4]**

Module	**Topics**
Module 1. Introduction To Data Security	● Data–Digital Building Blocks ● Importance of Data in the Information Age ● Threats to Data ● Data Security ● Potential Losses Due to Security Attacks ● Implementing Security
Module 2. Securing Operating Systems	● Guidelines to Secure Windows ● Guidelines to Secure Mac OS X
Module 3. Malware and Antiviruses	● What is Malware ● Types of Malware ● Symptoms of Malware Infection ● Antivirus ● Configuring and Using Antivirus Software ● How to Test If an Antivirus is Working
Module 4. Internet Security	● Understanding Web Browser Concepts ● Understanding IM Security ● Understanding Child Online Safety
Module 5. Security On Social Networking Sites	● Understanding Social Networking Concepts ● Understanding Various Social Networking Security Threats ● Understanding Facebook Security Settings ● Understanding Twitter Security Settings
Module 6. Securing Email Communications	● Understanding Email Security Concepts ● Understanding Various Email Security Threats ● Understanding Various Email Security Procedures
Module 7. Securing Mobile Devices	● Understanding Mobile Device Security Concepts ● Understanding Threats to a Mobile Device ● Understanding Various Mobile Security Procedures ● Understanding How to Secure iPhone and iPad Devices ● Understanding How to Secure Android Devices ● Understanding How to Secure Windows Device ● Mobile Security Tools
Module 8. Securing The Cloud	● The Concept of Cloud ● How Cloud Works ● Threats to Cloud Security ● Safeguarding Against Cloud Security Threats ● Cloud Privacy Issues

	● Addressing Cloud Privacy Issues ● Choosing a Cloud Service Provider
Module 9. Securing Network Connections	● Understanding Various Networking Concepts ● Understanding Setting Up a Wireless Network in Windows ● Understanding Setting Up a Wireless Network in Mac ● Understanding Threats to Wireless Network Security and Countermeasures ● Measures to Secure Network Connections
Module 10. Data Backup and Disaster Recovery	● Data Backup Concepts ● Types of Data Backups ● Windows Backup and Restore Procedures ● MAC OS X Backup and Restore Procedures ● Understanding Secure Data Destruction

Semester - III

BCO 315A	EC-Council Certified Security Specialist	4-0-0 [4]

Module 1	Information Security Fundamentals
Module 2	Networking Fundamentals
Module 3	Secure Network Protocols
Module 4	Information Security Threats and Attacks
Module 5	Social Engineering
Module 6	Hacking Cycle
Module 7	Identification, Authentication, and Authorization
Module 8	Cryptography
Module 9	Firewalls
Module 10	Intrusion Detection System
Module 11	Data Backup
Module 12	Virtual Private Network
Module 13	Wireless Network Security
Module 14	Web Security
Module 15	Ethical Hacking and Pen Testing
Module 16	Incident Response
Module 17	Computer Forensics Fundamentals
Module 18	Digital Evidence
Module 19	Understanding File Systems
Module 20	Windows Forensics
Module 21	Network Forensics and Investigating Network Traffic
Module 22	Steganography
Module 23	Analyzing Logs
Module 24	E-mail Crime and Computer Forensics
Module 25	Writing Investigative Report

Semester – IV

BCO 317A	Certified Network Defender	4-0-0 [4]

Module 01: Network Attacks and Defense Strategies	This module introduces you to different network-based attacks faced by the organization to understand their working and develop defense strategies.
Module 02: Administrative Network Security	It involves developing or updating security infrastructure and continuously monitoring networks for any suspicious actions or unauthorized access
Module 03: Technical Network Security	Implementing authentication and protection controls for user verification to avoid theft of sensitive information or data. Introducing the concept of zero trust and its effectiveness in maintaining a better security posture
Module 04: Network Perimeter Security	Implementation and management of perimeter devices like firewalls, Intrusion Detection Systems, Intrusion Prevention Systems
Module 05: Endpoint Security-Windows Systems	Security of end-user devices and entry points by implying endpoint security on Windows devices.
Module 06: Endpoint Security-Linux Systems	Securing entry points or end-user devices by ensuring endpoint security on Linux devices
Module 07: Endpoint Security-Mobile Devices	Securing entry points or end-user devices by ensuring endpoint security on mobile devices
Module 08: Endpoint Security-IoT Devices	Fundamentals of IoT, IoT threats and security using endpoint security implementation
Module 09: Administrative Application Security	Understanding the methodologies of administrative application security and its importance to minimize the security-related vulnerabilities in the application
Module 10: Data Security	Implementing policies to safeguard data from unauthorized access using various techniques like encryption, hashing, tokenization, and

	other key management practices. Concept of data storage, data classification, data masking, retention and destruction
Module 11: Enterprise Virtual Network Security	In-depth understanding of virtualization, related threats, and security. Essentials of software-defined network (SDN) security, network function virtualization (NFV) security
Module 12: Enterprise Cloud Network Security	Introduction to cloud computing, threats, challenges and security across cloud platforms, concepts of container security, docker security, and Kubernetes security
Module 13: Enterprise Wireless Network Security	Understanding of wireless network security essentials, threats, attacks, and countermeasures.
Module 14: Network Traffic Monitoring and Analysis	Analysis and monitoring of logs from various perimeter network devices to identify any anomalies in the traffic.
Module 15: Network Logs Monitoring and Analysis	Analyzing the events generated by various devices in the network to identify signs of any suspicious activity or a potential incident
Module 16: Incident Response and Forensic Investigations	Understanding of incident management response process and methodologies to be followed in case of security incidents. Understanding of forensics investigation techniques and tools used for analysis.
Module 17: Business Continuity and Disaster Recovery	Understanding the importance of BCP and DR, related concepts and procedures required to allow smooth functioning of operations in case of a disaster
Module 18: Risk Anticipation with Risk Management	Risk management process, analyzing various risks that the organization is susceptible to and developing policies to manage them.
Module 19: Threat Assessment with Attack Surface Analysis	Analyzing the threats and attack vectors to develop solutions for their countermeasures
Module 20: Threat Prediction with Cyber Threat Intelligence	Developing a proactive approach by understanding various frameworks aiding in threat intelligence to anticipate the kinds of attacks hackers could use to gain access to the network.

BCO 186A	Principle of Cryptography	3-0-0 [3]

OBJECTIVE:

- To gain knowledge about the mathematics of the cryptographic algorithms.
- To get an insight into the working of different existing cryptographic algorithms.
- To learn how to use cryptographic algorithms in security.

UNIT 1	Algebra: Group, cyclic group, cyclic subgroup, field, probability. Number Theory: Fermat's theorem , Cauchy 's theorem, Chinese remainder theorem, primality testing algorithm, Euclid's algorithm for integers, quadratic residues, Legendre symbol, Jacobi symbol etc..
UNIT 2	Cryptography and cryptanalysis, Classical Cryptography, substitution cipher, different type of attack: CMA,CPA,CCA etc, Shannon perfect secrecy, OTP, Pseudo random bit generators, stream ciphers and RC4.
UNIT 3	Block ciphers: Modes of operation, DES and its variants, AES, linear and differential cryptanalysis.
UNIT 4	One-way function , trapdoor one-way function, Public key cryptography, RSA cryptosystem, Diffie-Hellman key exchange algorithm, Elgamal Cryptosystem.
UNIT 5	Cryptographic hash functions, secure hash algorithm, Message authentication, digital signature, RSA digital signature, Elgamal digital signature.

Course Outcome*:*

CO1: Building a new unbreakable cryptosystem
CO2: Blending the existing cryptographic algorithms with the existing communication protocols
CO3: Analyzing and application of cryptography for secure e Commerce and other secret transactions

MAPPING COURSE OUTCOMES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES:

Course Outcome	**Program Outcome**												**Program Specific Outcome**		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	H											M	H	M	
CO2	H	H		L							L		H	M	
CO3	H	M	H		H						M		H		L

H = Highly Related; M = Medium L = Low

Textbook:

1. Stinson. D. Cryptography: Theory and Practice, third edition, Chapman & Hall/CRC, 2010.

Reference Books:

1. W. Stallings, Cryptography and Network Security Principles and practice, 5/e, Pearson Education Asia, 2012.
2. Behrouz A. Forouzan and Debdeep Mukhopadhyay, Cryptography and Network Security, second edition, Tata McGraw Hill, 2011
3. Thomas Koshy, Elementary Number Theory with applications, Elsevier India, 2005.

Semester – V

BCO 319A	Certified Ethical Hacker	4-0-0 [4]

Module 01: Introduction to Ethical Hacking	This module introduces you to the basic concepts of hacking, what is hacking, who are hackers, their intent, and other related terminologies. The next modules dive deeper into the various phases of hacking, which would help you in thinking with the mindset of a hacker.
Module 02: Footprinting and Reconnaissance	Gathering information from various sources using footprinting tools and how to defend against the same.
Module 03: Scanning Networks	Different techniques to identify and scan the network, host, and port discovery by utilizing various scanning tools.
Module 04: Enumeration	Finding detailed information about the hosts and ports discovered during scanning. This module now includes sub-domains like NFS enumeration and related tools, DNS cache snooping, and DNSSEC Zone walking, along with the countermeasures.
Module 05: Vulnerability Analysis	It introduces the concepts of vulnerability assessment, its types, along with a hands-on experience of tools that are currently used in the industry.
Module 06: System Hacking	It focuses on the "how" part. How to gain access of the system, how to escalate privileges, how to maintain access, and how to clear your tracks. The next modules help to develop a deeper understanding of various defense and attack methodologies and concepts that aid the process of hacking.
Module 07: Malware Threats	Malware threat terminologies, viruses, worms, trojans, their analysis, and countermeasures to prevent data loss. The introduction and analysis of malware like, Emotet and fileless that are gaining popularity have been updated under this section. APT concepts have also been added.
Module 08: Sniffing	Packet sniffing techniques, associated tools, and related defensive techniques.
Module 09: Social Engineering	Since humans are the most significant vulnerability for any organization, it becomes essential to understand how attackers use them for their purpose for carrying out attacks like identity theft, impersonation, insider threat, and how to defend against such social engineering attacks.
Module 10: Denial-of-Service	As DoS and DDoS are some of the most common purposes of attackers, this module talks about these attacks, use cases, and the related attack and defense tools.
Module 11: Session Hijacking	To provide a deeper understanding of the technique, its purpose, tools used along with the countermeasures.

Module 12: Evading IDS, Firewalls, and Honeypots	Understand the terminologies and working of these inline defenses and techniques to learn how to evade these while performing an attack.
Module 13: Hacking Web Servers	Web servers based attacks, methodologies, tools used, and defense
Module 14: Hacking Web Applications	Web application-based attacks, techniques, and mitigation.
Module 15: SQL Injection	An in-depth understanding of the top OWASP top 10 web app vulnerability, it's working and the mitigation.
Module 16: Hacking Wireless Networks	Wireless encryption, wireless hacking, and Bluetooth hacking-related concepts
Module 17: Hacking Mobile Platforms	Management of mobile devices, mobile platform attack vectors, and vulnerabilities related to Android and iOS systems
Module 18: IoT Hacking	Recognizing the vulnerabilities in IoT and ensuring the safety of IoT devices. Operational Technology (OT) essentials, introduction to ICS, SCADA, and PLC, threats, attack methodologies, and attack prevention. The concept of OT is a new addition.
Module 19: Cloud Computing	Cloud computing, threats, and security. Additionally, the essentials of container technology and serverless computing have been added.
Module 20: Cryptography	Encryption algorithms, Public Key Infrastructure (PKI), cryptographic attacks, and cryptanalysis.

BCO 188A	Cyber Forensic & investigation	3-0-0 (3)

Objective:

- To study the fundamentals of Computer Forensics

• To learn, analyze and validate Forensics Data
• To study the tools and tactics associated with Cyber Forensics

UNIT 1	File systems, Microsoft file structure, Examining NTFS disks, Microsoft BitLocker, Third Party Disk Encryption Tools, Windows Registry, Start-up Tasks, Virtual Machines, Macintosh file structure and boot process, UNIX and Linux disk structures and boot processes. Other Disk structures (CD, SCSI, IDE and SATA devices)
UNIT 2	Commercial Forensic Tools (Encase, FTK), Advanced Features of forensic tools (search, encryption and decryption, data carving), windows registry, memory analysis, advanced file system analysis (deleted and hidden data, metadata, temporary file, unknown\executable file analysis), applied decryption.
UNIT 3	Graphic files: recognition, lossless and lossy data compression, locating and recovering graphic files, Identifying unknown file formats.
UNIT 4	Virtual Machines, Network Forensics, Network tools, E-mail Investigation, E-mail forensics tools, Mobile Device Forensic.
UNIT 5	Computer Investigation,Evidence acquisition, Processing crime and Incidence scene, Preserving, Analysis, Digital forensic investigation procedures, Report writing, Ethics

OUTCOMES: At the end of the course, the student should be able to:
CO1: Understand the fundamentals of Computer Forensics
CO2: Learn the issues of Data Acquisition and Data Recovery
CO3: Explore networking in cyber forensics
CO4: Learn to analyze and validate forensics data
CO5: Be familiar with forensic tools and case studies

MAPPING COURSE OUTCOMES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES:

Course Outcome	**Program Outcome**												**Program Specific Outcome**		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	H	M		H									H		
CO2	H	H				M						H	H	L	
CO3	H	H		H									M		
CO4	H	M	H		M	L		M				M		M	H
CO5	M		H		H						L				H

H = Highly Related; M = Medium L=Low

Text Books –

1. Computer Evidence - Collection and Preservation.Brown, C.L.T. Course Technology CENGAGE Learning.
2. Guide to Computer Forensics And Investigations Nelson, Bill ; Phillips, Amelia; Enfinger, Frank; Steuat, Christopher Thomson Course Technology.
3. Scene of the Cybercrime. Shinder, Debra Littlejohn and Tittel, Syngress

Reference Books:

1. Computer Forensics – Computer Crime Scene Investigation.Vacca, John R. Charles River Media
2. Bunting, Steve and William Wei. EnCase Computer Forensics: The Official EnCE: EnCase Certifed Examiner Study Guide. Sybex, 2006
3. Prosise, Chris, Kevin Mandia, and Matt Pepe. Incident Response: Computer Forensics. McGraw-Hill,
4. Casey, Eoghan, ed. Handbook of Computer Crime Investigation, Forensic Tools and Technology, Academic press
5. Carrier, Brian. File System Forensic Analysis. Addison-Wesley Professional

BCO 189A	Web and Android Security	3-0-1 [4]

OBJECTIVES:

- Introduce the concept of web application security concerns and its related issues.
- To familiarize the students with various types of analysis techniques ,attacks and tools.
- To introduce the various android application architecture and Security concerns.
- To introduce the various types of mobile attacks.

UNIT 1	Web applications: Introduction to web applications, Web application hacking, Overview of browsers, extensions, and platforms.Attacks, detection evasion techniques, and countermeasures for the most popular web platforms, including IIS, Apache, PHP, and ASP.NET Attacks and countermeasures for common web authentication mechanisms, including password-based, multifactor (e.g., CAPTCHA), and online authentication services like Windows Live ID.
UNIT 2	Advanced session analysis, hijacking, and fixation techniques, cross-site scripting, SQL injection, classic categories of malicious input, Overlong input (like buffer overflows), canonicalization attacks (like the infamous dot-dot-slash), and meta characters (including angle brackets, quotes, single quote, double dashes, percent, asterisk, underscore, newline, ampersand, pipe, and semicolon), beginner-to-advanced SQL injection tools and techniques, stealth-encoding techniques and input validation/ output-encoding countermeasures.
UNIT 3	Introduction to Android Applications and Mobile App Security: History of Android, Understanding Android Hardware and Software Architecture, Understanding Android Security Model. Understanding Android Permission Model for Application Security, Sandboxing, Codesigning, Encryption, rooting Devices, Understanding APK Understanding Directories and Files on an APK 9
UNIT 4:	Mobile Application Attacks 1: Setting up Mobile App Pentesting Environment,Interact with the Devices, Starting with Drozer,Understanding AndroidManifest.xml,Configuring, Burp and Traffic Interception,Traffic Interception Bypass, Weak Server Side Controls,Insecure Data Storage,Insufficient Transport Layer Protection,Unintended Data Leakage,Poor Authentication & Authorization 10
UNIT 5	Mobile Application Attacks 2: Broken Cryptography,Client Side Injections,Security Decisions via Untrusted Input,Improper Session Handling,Lack of Binary Protection,Exploiting Debuggable Applications,Developer Backdoor,Location spoofing to download location restricted apps,Configuring Live Device for Penetration Testing,Mitigation Approach for all Vulnerabilities.

OUTCOMES:-

Upon completion of this course, the student will be able to:

CO1: Learn web application security concerns and its related issues.
CO2: Develop the Secure web application with help various of analysis techniques and knowledge of different attacks and tools.
CO3: Understand android application architecture and Security issues.
CO4: Know about various types of mobile attacks and to deal with these attacks and develop the secure application

MAPPING COURSE OUTCOMES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES:

Course Outcome	**Program Outcome**												**Program Specific Outcome**		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	H	H		M									H		L
CO2	H	H	H		M	L				L		L	H	M	
CO3	H			L	M		L		L				H		M
CO4	H		H			L				M		L		M	

Text Books:

1. Hacking Exposed Web Applications, 3rd edition, JOEL SCAMBRAY, VINCENT LIU, CALEB SIMA
2. The Web Application Hacker's Handbook Discovering and Exploiting Security Flaws By Dafydd Stuttard, Marcus Pinto
3. Mobile device security: A comprehensive guide to securing your information in a moving world. Boca Raton, FL: Auerbach Publications - Fried, S.

Reference Books:

1. Rich Bowen, Ken Coar, "Apache Cookbook", O'Reilly
2. Open Web Application Security Project. A Guide to Building Secure Web Applications and Web Services. http://www.owasp.org/index.php/Category:OWASP_Guide_Project
3. 2 The web application hacker's handbook: Discovering and exploiting security flaws (2nd ed.). Indianapolis, IN: Wiley, John & Sons - Stuttard, D. & Pinto, M.
4. Mobile application security. New York: McGraw-Hill Companies - Dwivedi, H., Clark, C., &Thiel, D.

Department Elective 6

BCO 183A	XML Programming	3-0-1

Course Objectives

1. To help students understand the role of xml in interoperability of applications.

2. To help students to have complete understanding of publishing and applying xml.

3. To help students understand XML in detail w.r.t its fundamentals, syntax

4. Understand the use and role of web services.

5. To help students understand the working of CSS and AJAX in web-based applications.

UNIT 1	Unit-1 Introduction to XML Why XML?, Extending and Adopting Markup Languages, From SGML to XML and XHTML, Benefits and Drawbacks of XML. XML FUNDAMENTALS: Creating an XML Document, Defining Structure, Rules for Well-Formed and Valid XML, Changing XML Documents XML SYNTAX : Tag Attributes and Naming Rules, Empty and Non-Empty Elements, Processing Instructions for XML, Accessing Data from XML Elements.
UNIT 2	Unit-2 XML DOCUMENT TYPE DEFINITION (DTD) XML DTD as an XML Schema, Creating a DTD, Element Conditions and Quantifiers, Referencing DTD Declarations, Validating DTD Compliance
UNIT 3	Unit-3 XML SCHEMA DEFINITION (XSD),Element and Attribute Declarations, Simple, Complex, and Built-in Types, Named and Anonymous Types, Associating XML with a Schema, Validating XSD Compliance
UNIT 4	Unit-4 PUBLISHING XML AND APPLYING XML Stylesheet Languages, Using Style Sheets with XML,Page Layout with Cascading Style Sheets (CSS), CSS Syntax and Classes APPLYING XML: XML and Web Services, HTML with XML, XML and eCommerce, Storing Binary Data in XML Publish and Apply XML : Stylesheet Languages, What is CSS? , Using stylesheet with XML, Layout with cascading style sheet(css), css syntax and classes. Xml and web services, HTML, XML and eCommerce, Storing Binary Data in XML.
UNIT 5	Unit-5 CSS AND AJAX 5 CSS: Introduction, CSS and HTML, CSS Essentials, Typography, Colors and Backgrounds AJAX: Security, Performance, Dynamic double combo, The enhanced Ajax web portal, Live search using XSLT, Building stand-alone

	applications with Ajax.

Course Outcomes

CO1. A complete knowledge of XML and its structure
CO2. Detailed understanding of xml syntax and how to write them.
CO3. Detailed understanding of XML SCHEMA and the uses of DTD and how to write them and integrate with XML data
CO4: To have complete understanding of publishing and applying xml.
CO5:To have complete understanding of the benefits and the implementation of CSS and AJAX in web based applications

MAPPING COURSE OUTCOMES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES:

Course Outcomes	**Program Outcomes**												**Program specific Outcomes**		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	M											L	L		
CO2	L	M	M	L	M									M	
CO3		L	L	M	M								M	M	M
CO4		M	L		L							L			L
CO5	L	H	M	L	H							M	H		H

Text Books

1. XML: The Complete Reference, Heather Williamson, TMH

2. PHP: The Complete Reference, Steven Holzner, TMHH

Reference Books

1. XML How to Program, H. M. Deitel, P. J. Deitel, Pearson

2. Learning XML, Erik T. Ray, OReilly

BCO 191A	Application of AI in Cyber Security	3-0-0

OBJECTIVE:

- To study various AI terminologies in Cyber security
- Understand the various threats and attacks in cyber world
- To be familiar with different types of attacks and AI techniques to detect them
- Study and Compare real-world attacks and AI to solve them
- To understand ethical challenges and enforcements of laws in Cyber attacks

UNIT 1	Introduction of AI in Cyber Security: AI, Machine learning, and Deep learning within cyber security, What AI and machine learning can do for cyber security, How AI is used in cyber security, Examples of machine learning in cyber security, Use of Artificial Intelligence in Cyber Security, The Future of Cyber security, Impact of AI on Cyber security, How They Will Shape the Future. AI systems' support to cyber security, Major techniques in the use of AI for system robustness, resilience, and response,
UNIT 2	Cyber security for AI : Classification of AI Attacks based on attack motivation, Integrity Attack, Availability Attack, Replication Attack, Confidentiality Attack , Classification of AI attacks based on target ,Classification of AI attacks based on attacker capabilities ,Handling AI Attack, Social Media Attacks , Secure AI , Available Software Resources. Case Study of Cybercrime: Official Website of Maharashtra Government Hacked, Indian Banks Lose Millions of Rupees, Parliament Attack, Pune City Police Bust Nigerian Racket, E-mail spoofing instances, The Indian Case of online Gambling, An Indian Case of Intellectual Property Crime, Financial Frauds in Cyber Domain.
UNIT 3	AI Techniques for Cyber Security : Introduction, Malware Detection and Analysis, Intrusion Detection Systems (IDS) , Generative Adversarial Networks, Attack Detection , Trustworthiness of data, Artificial Intelligence and Hardware Security, Consideration for adoption of AI , Typical use cases.
UNIT 4	**Applications from real world: Study of some applications** AI-powered threat detection, Detection of sophisticated cyber-attacks, Reducing Threat Response Time **, AI-based Antivirus Software, Fighting AI Threats, Email Monitoring ,**Using machine learning to analyze mobile endpoints, to enhance human analysis and automate repetitive security tasks.
UNIT 5	Ethics and Laws in Applications of AI in Cyber world :Ethical considerations related to AI in cyber security, Standards on Cyber Security Using AI ,Current and future AI laws: accountability, audit ability, and regulatory enforcement, Existing legal frameworks in cyber security and major policy issues, Risk-assessment policies and suitability testing, privacy and data governance , **Pitfalls of AI in cyber law.**

Course Outcome*:*

CO1. Understand role of AI in Cyber Security
CO2. Understand various threats and attacks in cyber world
CO3. Compare and analyze types of attacks and AI techniques to detect them
CO4. Understand ethical challenges and enforcements of laws for Cyber Security

MAPPING COURSE OUTCOMES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES:

Course Outcome	**Program Outcome**												**Program Specific Outcome**		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	H	M										H			
CO2	M	M										H			
CO3	H	H										H	L	M	
CO4	M	M						M				H			

H = Highly Related; M = Medium; L = Low

Text Book:

1. Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley

2. B. B. Gupta, D. P. Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335, 2018

Information Security
Department Elective 8

BCO 192A	Block chain and Cryptocurrency Technology	3-0-1 [4]

OBJECTIVES:

- This course is to understand Blockchain and its main application cryptocurrency.
- Students will learn how this system works and how can they utilize and what application can be build.

UNIT 1	Basics: Distributed Database, Two General Problem, Byzantine General problem and Fault Tolerance, Hadoop Distributed File System, Distributed Hash Table, ASIC resistance, Turing Complete. ,Cryptography: Hash function, Digital Signature - ECDSA, Memory Hard Algorithm, Zero Knowledge Proof
UNIT 2	Blockchain: Introduction, Advantage over conventional distributed database, Blockchain Network, Mining Mechanism, Distributed Consensus, Merkle Patricia Tree, Gas Limit, Transactions and Fee, Anonymity, Reward, Chain Policy, Life of Blockchain application, Soft & Hard Fork, Private and Public blockchain.
UNIT 3	Distributed Consensus: Nakamoto consensus, Proof of Work, Proof of Stake, Proof of Burn, Difficulty Level, Sybil Attack, Energy utilization and alternate
UNIT 4:	Cryptocurrency: History, Distributed Ledger, Bitcoin protocols - Mining strategy and rewards, Ethereum - Construction, DAO, Smart Contract, GHOST, Vulnerability, Attacks, Sidechain, Name coin Cryptocurrency Regulation: Stakeholders, Roots of Bitcoin, Legal Aspects - Cryptocurrency Exchange, Black Market and Global Economy.
UNIT 5	Blockchain Applications: Internet of Things, Medical Record Management System, Domain Name Service and future of Blockchain.

OUTCOMES:-

Upon completion of this course, the student will be able to:

CO1: Learn basic concepts of block-chains
CO2: Understanding the crypto-currency technology
CO3: Know the block chain architecture
CO4: Study the block chain applications
CO5: Learn the regulatory frameworks

MAPPING COURSE OUTCOMES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES:

Course Outcome	Program Outcome												Program Specific Outcome		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	H		L		L		M								
CO2	L	L											L		
CO3	M				L		M	M							
CO4	M		l					M					L	M	
CO5							M								L

Reference Books:

- Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press (July 19, 2016).
- Wattenhofer, The Science of the Blockchain
- Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies
- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System
- DR. Gavin Wood, "ETHEREUM: A Secure Decentralized Transaction Ledger,"Yellow paper.2014.
- Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli, A survey of attacks on Ethereum smart contracts

Tutorial & Practical

- Naive Blockchain construction,
- Memory Hard algorithm –
- Hashcash implementation,
- Direct Acyclic Graph,
- Play with Go-Ethereum,
- Smart Contract Construction,
- Toy application using Blockchain,

Mining puzzles