JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech. COMPUTER NETWORKS AND INFORMATION SECURITY/ COMPUTER NETWORKS/CYBER SECURITY
EFFECTIVE FROM ACADEMIC YEAR 2022 - 23 ADMITTED BATCH

R22 COURSE STRUCTURE AND SYLLABUS

I YEAR I – SEMESTER

Course Code	Course Title	L	T	P	Credits
Professional Core - I	Advanced Computer Networks	3	0	0	3
Professional Core - II	Advanced Data Structures	3	0	0	3
Professional Elective - I	1. Information Security 2. Vulnerability Assessment & Penetration Testing 3. Mobile Application Security	3	0	0	3
Professional Elective - II	1. Network Coding Theory 2. Advanced Wireless Networks 3. Digital Forensics	3	0	0	3
Lab - I	Advanced Data Structures Lab	0	0	4	2
Lab - II	Professional Elective - I Lab	0	0	4	2
	Research Methodology &IPR	2	0	0	2
Audit - I	Audit Course- I	2	0	0	0
	Total	**16**	**0**	**8**	**18**

Professional Elective- I and Professional Elective- I Lab must be of same course.

I YEAR II – SEMESTER

Course Code	Course Title	L	T	P	Credits
Professional Core - III	Distributed Systems	3	0	0	3
Professional Core - IV	Web & Database Security	3	0	0	3
Professional Elective - III	1. Intrusion Detection & Prevention Systems 2. Cloud Security 3. Blockchain Technology	3	0	0	3
Professional Elective - IV	1. Digital Payment Systems 2. User Authentication Techniques 3. Data Analytics for Fraud Detection	3	0	0	3
Lab - III	Web & Database Security Lab	0	0	4	2
Lab - IV	Professional Elective - III Lab	0	0	4	2
	Mini Project with Seminar	0	0	4	2
Audit - II	Audit Course- II	2	0	0	0
	Total	**14**	**0**	**12**	**18**

Professional Elective- III and Professional Elective- III Lab must be of same course.

II YEAR I – SEMESTER

Course Code	Course Title	L	T	P	Credits
Professional Elective - V	1. Cyber Security 2. Network Management Systems and Operations 3. Vehicular Ad-Hoc Networks	3	0	0	3
Open Elective	Open Elective	3	0	0	3
Dissertation	Dissertation Work Review -II	0	0	12	6
	Total	**6**	**0**	**12**	**12**

II YEAR II - SEMESTER

Course Code	Course Title	L	T	P	Credits
Dissertation	Dissertation Work Review -III	0	0	12	6
Dissertation	Dissertation Viva-Voce	0	0	28	14
	Total	**0**	**0**	**40**	**20**

Note: For Dissertation Work Review - I, Please refer 7.10 in R22 Academic Regulations.

Audit Course I&II:

1. English for Research Paper Writing
2. Disaster Management
3. Sanskrit for Technical Knowledge
4. Value Education
5. Constitution of India
6. Pedagogy Studies
7. Stress Management by yoga
8. Personality Development Through Life Enlightenment Skills

Open Electives for other Departments:

1. IPR
2. Fault Tolerance Systems
3. Intrusion Detection Systems
4. Digital Forensics
5. Optimization Techniques
6. Cyber Physical Systems
7. Graph Analytics

ADVANCED COMPUTER NETWORKS (PC - I)

M.Tech CNIS/CN/CYS I Year I Sem.

L	T	P	C
3	0	0	3

Prerequisites: Data Communication, Basic Networking Principles, Computer Networks

Course Objective: This course aims to provide advanced background on relevant computer networking topics to have a comprehensive and deep knowledge in computer networks.

Course Outcomes:

1. Understanding of holistic approach to computer networking
2. Ability to understand the computer network protocols and their applications
3. Ability to design simulation concepts related to packet forwarding in networks.

UNIT - I

Data-link protocols: Ethernet, Token Ring and Wireless (802.11). Wireless Networks and Mobile IP: Infrastructure of Wireless Networks, Wireless LAN Technologies, IEEE 802.11 Wireless Standard, Cellular Networks, Mobile IP, Wireless Mesh Networks (WMNs), Multiple access schemes Routing and Internetworking: Network–Layer Routing, Least-Cost-Path algorithms, Non-Least-Cost-Path algorithms, Intra-domain Routing Protocols, Inter-domain Routing Protocols, Congestion Control at Network Layer.

UNIT - II

Transport and Application Layer Protocols: Client-Server and Peer-To-Peer Application Communication, Protocols on the transport layer, reliable communication. Routing packets through a LAN and WAN. Transport Layer, Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Mobile Transport Protocols, TCP Congestion Control. Principles of Network Applications,

UNIT- III

The Web and HTTP, File Transfer: FTP, Electronic Mail in the Internet, Domain Name System (DNS), P2P File Sharing, Socket Programming with TCP and UDP, building a Simple Web Server Creating simulated networks and passing packets through them using different routing techniques. Installing and using network monitoring tools.

UNIT - IV

Wireless and Mobile Networks: Introduction, Wireless links and Network Characteristics - CDMA, Wifi: 802.11 Wireless LANS, Cellular internet access, Mobility management: Principles

UNIT - V

Multimedia networking: Multimedia networking applications, streaming stored video, Voice-over-IP, Protocols for real-time conversational applications.

TEXT BOOKS:

1. Computer Networking: A Top-Down Approach, James F. Kuros and Keith W. Ross, Pearson, 6th Edition, 2012.
2. Computer Networks and Internets, Duglas E. Comer, 6th Edition, Pearson.

REFERENCES:

1. A Practical Guide to Advanced Networking, Jeffrey S. Beasley and Piyasat Nilkaew, Pearson, 3rd Edition, 2012
2. Computer Networks, Andrew S. Tanenbaum, David J. Wetherall, Prentice Hall.

ADVANCED DATA STRUCTURES (PC - II)

M.Tech CNIS/CN/CYS I Year I Sem.

L	T	P	C
3	0	0	3

Prerequisites: A course on "Data Structures"

Course Objectives

1. Introduces the heap data structures such as leftist trees, binomial heaps, Fibonacci and min-max heaps
2. Introduces a variety of data structures such as disjoint sets, hash tables, search structures and digital search structures

Course Outcomes

1. Ability to select the data structures that efficiently model the information in a problem
2. Ability to understand how the choice of data structures impact the performance of programs
3. Design programs using a variety of data structures, including hash tables, search structures and digital search structures

UNIT - I

Heap Structures

Introduction, Min-Max Heaps, Leftist trees, Binomial Heaps, Fibonacci heaps.

UNIT - II

Hashing and Collisions

Introduction, Hash Tables, Hash Functions, different Hash Functions: Division Method, Multiplication Method, Mid-Square Method, Folding Method, Collisions

UNIT - III

Search Structures: OBST, AVL trees, Red-Black trees, Splay trees,
Multiway Search Trees: B-trees, 2-3 trees

UNIT - IV

Digital Search Structures

Digital Search trees, Binary tries and Patricia, Multiway Tries, Suffix trees, Standard Tries, Compressed Tries

UNIT - V

Pattern matching

Introduction, Brute force, the Boyer –Moore algorithm, Knuth-Morris-Pratt algorithm, Naïve String, Harspool, Rabin Karp

TEXT BOOKS:

1. Fundamentals of data structures in C++ Sahni, Horowitz, Mehatha, Universities Press.
2. Introduction to Algorithms, TH Cormen, PHI

REFERENCES:

1. Design methods and analysis of Algorithms, SK Basu, PHI.
2. Data Structures & Algorithm Analysis in C++, Mark Allen Weiss, Pearson Education.
3. Fundamentals of Computer Algorithms, 2nd Edition, Ellis Horowitz, Sartaj Sahni, Sanguthevar Rajasekaran, Universities Press.

INFORMATION SECURITY (Professional Elective - I)

M.Tech CNIS/CN/CYS I Year I Sem.

L	T	P	C
3	0	0	3

Prerequisites

1. A Course on "Computer Networks and a course on Mathematics

Course Objectives

1. To understand the fundamentals of Cryptography
2. To understand various key distribution and management schemes
3. To understand how to deploy encryption techniques to secure data in transit across data networks
4. To apply algorithms used for secure transactions in real world applications

Course Outcomes

1. Demonstrate the knowledge of cryptography, network security concepts and applications.
2. Ability to apply security principles in system design.
3. Ability to identify and investigate vulnerabilities and security threats and mechanisms to counter them.

UNIT - I

Security Attacks (Interruption, Interception, Modification and Fabrication), Security Services (Confidentiality, Authentication, Integrity, Non-repudiation, access Control and Availability) and Mechanisms, A model for Internetwork security.

Classical Encryption Techniques, DES, Strength of DES, Differential and Linear Cryptanalysis, Block Cipher Design Principles and Modes of operation, Blowfish, Placement of Encryption Function, Traffic Confidentiality, key Distribution, Random Number Generation.

UNIT - II

Public key Cryptography Principles, RSA algorithm, Key Management, Diffie-Hellman Key Exchange, Elliptic Curve Cryptography.

Message authentication and Hash Functions, Authentication Requirements and Functions, Message Authentication, Hash Functions and MACs Hash and MAC Algorithms SHA-512, HMAC.

UNIT - III

Digital Signatures, Authentication Protocols, Digital signature Standard, Authentication Applications, Kerberos, X.509 Directory Authentication Service.

Email Security: Pretty Good Privacy (PGP) and S/MIME.

UNIT - IV

IP Security:

Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management.

Web Security: Web Security Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET).

UNIT - V

Intruders, Viruses and Worms Intruders, Viruses and related threats Firewalls: Firewall Design Principles, Trusted Systems, Intrusion Detection Systems.

TEXT BOOK:

1. Cryptography and Network Security (principles and approaches) by William Stallings Pearson Education, 4th Edition.

REFERENCE BOOKS:

1. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education.
2. Principles of Information Security, Whitman, Thomson.

VULNERABILITY ASSESSMENT AND PENETRATION TESTING (Professional Elective - I)

M.Tech CNIS/CN/CYS I Year I Sem.

L	T	P	C
3	0	0	3

Pre-requisites:

1. Knowledge in information security.
2. Knowledge on Web Application.

Course Objectives:

1. Give an introduction to Vulnerability Assessment and Penetration Testing.
2. To be familiar with the Penetration Testing and Tools.
3. To get an exposure to Metasploit exploitation tool, Linux exploit and Windows exploit.
4. To gain knowledge on Web Application Security Vulnerabilities, Vulnerability analysis and Malware analysis.

Course Outcomes:

1. Understand social engineering attacks
2. Learn to handle the vulnerabilities of a Web application.
3. Perform penetration testing
4. Analyze the malware type and impact.

UNIT-I

Introduction Ethics of Ethical Hacking: Why you need to understand your enemy's tactics, recognizing the gray areas in security, Vulnerability Assessment and Penetration Testing. Penetration Testing and Tools: Social Engineering Attacks: How a social engineering attack works, conducting a social engineering attack, common attacks used in penetration testing, preparing yourself for face-to-face attacks, defending against social engineering attacks.

UNIT-II

Physical Penetration Attacks: Why a physical penetration is important, conducting a physical penetration, Common ways into a building, Defending against physical penetrations. Insider Attacks: Conducting an insider attack, Defending against insider attacks. Metasploit: The Big Picture, Getting Metasploit, Using the Metasploit Console to Launch Exploits, Exploiting Client-Side Vulnerabilities with Metasploit, Penetration Testing with Metasploit's Meterpreter, Automating and Scripting Metasploit, Going Further with Metasploit.

UNIT-III

Managing a Penetration Test: planning a penetration test, structuring a penetration test, execution of a penetration test, information sharing during a penetration test, reporting the results of a Penetration Test. Basic Linux Exploits: Stack Operations, Buffer Overflows, Local Buffer Overflow Exploits, Exploit Development Process. Windows Exploits: Compiling and Debugging Windows Programs, Writing Windows Exploits, Understanding Structured Exception Handling (SEH), Understanding Windows Memory Protections (XPSP3, Vista, 7 and Server 2008), Bypassing Windows Memory Protections.

UNIT-IV

Web Application Security Vulnerabilities: Overview of top web application security vulnerabilities, Injection vulnerabilities, cross-Site scripting vulnerabilities, the rest of the OWASP Top Ten SQL Injection vulnerabilities, Cross-site scripting vulnerabilities. Vulnerability Analysis: Passive Analysis, Source Code Analysis, Binary Analysis.

UNIT-V

Client-Side Browser Exploits: Why client-side vulnerabilities are interesting, Internet explorer security concepts, history of client- side exploits and latest trends, finding new browser-based vulnerabilities

heap spray to exploit, protecting yourself from client-side exploit. Malware Analysis: Collecting Malware and Initial Analysis: Malware, Latest Trends in Honeynet Technology, Catching Malware: Setting the Trap, Initial Analysis of Malware.

TEXT BOOKS:

1. Gray Hat Hacking-The Ethical Hackers Handbook", Allen Harper, Stephen Sims, Michael Baucom, 3rd Edition, Tata Mc Graw-Hill.
2. The Web Application Hacker's Handbook-Discovering and Exploiting Security flaws", Dafydd Suttard, Marcus pinto, 1st Edition, Wiley Publishing.

REFERENCES:

1. Penetration Testing: Hands-on Introduction to Hacking, Georgia Weidman, 1st Edition, No Starch Press.
2. The Pen Tester Blueprint-Starting a Career as an Ethical Hacker, L. Wylie, Kim Crawly, 1st Edition, Wiley Publications.

MOBILE APPLICATION SECURITY (Professional Elective - I)

M.Tech CNIS/CN/CYS I Year I Sem.

L	T	P	C
3	0	0	3

Course Objectives: This course provides a thorough understanding of mobile platforms, including attack surfaces, risk landscape & more.

Course Outcomes:

1. Understand common mobile application security vulnerabilities
2. Define the security controls of multiple mobile operating systems
3. Understand and analyze Bluetooth technology
4. understand and analyze overview of SMS security and Enterprise security

UNIT-I

Top Mobile Issues and Development Strategies: Top Issues Facing Mobile Devices, Physical Security, Secure Data Storage (on Disk), Strong Authentication with Poor Keyboards , Multiple-User Support with Security, Safe Browsing Environment , Secure Operating Systems, Application Isolation, Information Disclosure, Virus, Worms, Trojans, Spyware, and Malware , Difficult Patching/Update Process, Strict Use and Enforcement of SSL, Phishing , Cross-Site Request Forgery (CSRF), Location Privacy/Security, Insecure Device Drivers, Multi Factor Authentication, Tips for Secure Mobile Application Development .

UNIT-II

WAP and Mobile HTML Security WAP and Mobile HTML Basics, Authentication on WAP/Mobile HTML Sites, Encryption, Application Attacks on Mobile HTML Sites, Cross-Site Scripting, SQL Injection, Cross-Site Request Forgery, HTTP Redirects, Phishing, Session Fixation, Non-SSL Login, WAP and Mobile Browser Weaknesses, Lack of HTTPOnly Flag Support, Lack of SECURE Flag Support, Handling Browser Cache, WAP Limitations.

UNIT-III

Bluetooth Security Overview of the Technology , History and Standards , Common Uses , Alternatives , Future, Bluetooth Technical Architecture , Radio Operation and Frequency, Bluetooth Network Topology , Device Identification , Modes of Operation , Bluetooth Stack ,Bluetooth Profiles, Bluetooth Security Features , Pairing , Traditional Security Services in Bluetooth, Security “Non-Features” , Threats to Bluetooth Devices and Networks, Bluetooth Vulnerabilities, Bluetooth Versions Prior to v1.2, Bluetooth Versions Prior to v2.1. Security for 1g Wi-Fi Applications, Security for 2g Wi-Fi Applications, Recent Security Schemes for Wi-Fi Applications

UNIT-IV

SMS Security Overview of Short Message Service, Overview of Multimedia Messaging Service, Wireless Application Protocol (WAP), Protocol Attacks, Abusing Legitimate Functionality, Attacking Protocol Implementations, Application Attacks, iPhone Safari, Windows Mobile MMS, Motorola RAZR JPG Overflow, Walkthroughs, Sending PDUs, Converting XML to WBXML.

UNIT-V

Enterprise Security on the Mobile OS Device Security Options, PIN, Remote, Secure Local Storage, Apple iPhone and Keychain, Security Policy Enforcement, Encryption, Full Disk Encryption, E-mail Encryption, File Encryption, Application Sandboxing, Signing, and Permissions, Application Sandboxing, Application Signing, Permissions, Buffer Overflow Protection, Windows Mobile, iPhone, Android, BlackBerry, Security Feature Summary.

TEXT BOOK:

1. Mobile Application Security, Himanshu Dwivedi, Chris Clark, David Thiel, TATA McGraw-Hill.

REFERENCES:

1. Mobile and Wireless Network Security and Privacy, Kami S. Makki,et al, Springer.
2. Android Security Attacks Defenses, Abhishek Dubey, CRC Press.

NETWORK CODING THEORY (Professional Elective - II)

M.Tech CNIS/CN/CYS I Year I Sem.

L	T	P	C
3	0	0	3

Course Objectives:

1. Learn the fundamentals of network coding theory.
2. Understand the performance parameters required for network coding.
3. Gain the knowledge of the network coding design methods.
4. Learn different approaches for the network coding.
5. Understand error correction and detection methods of adversarial errors.

Course Outcomes:

1. Demonstrate knowledge and understanding of the fundamentals of Network Coding Theory.
2. Summarize all the performance parameters and resources for network coding.
3. Construct the network code for different networks.
4. Deal with different approaches of Network Coding in lossy and lossless networks.
5. Deal with multiple sources network coding and detect adversarial errors.

UNIT - I

Introduction: A historical Perspective, Network Coding; Network Coding Benefits: Throughput, Robustness, Complexity, Security; Network Model.

Main Theorem of Network Multicast: The Min-Cut Max-flow Theorem, The Main network coding Theorem,

Theoretical Framework for Network Coding: A Network Multicast Model, algebraic Framework, Combinatorial Framework, Information-Theoretic Framework, Types of Routing and coding**.**

UNIT - II

Throughput Benefits of Network Coding: Throughput Measures, Linear Programming Approach, Configurations with Large Network Coding Benefits, Configurations with Small Network Coding Benefits, Undirected Graphs.

Networks with Delay and Cycles: Dealing with Delay, Optimizing for Delay, Dealing with Cycles.

Resources for Network Coding: Bounds on Code Alphabet Size, Bounds on the Number of Coding Points, Coding with Limited Resources.

UNIT - III

Network Code Design Methods For Multicasting: Common initial procedure, centralized algorithms, decentralized algorithms, scalability to network changes.

Single-Source Linear Network Coding:

Acyclic Networks: Acyclic Networks, Linear network code, Desirable properties of a linear network code, Existence and construction, Algorithm refinement for multicast.

Cyclic Networks: Delay-Free Cyclic Code, Non-equivalence between local and global descriptions, Convolutional network code, decoding of convolutional network code.

UNIT - IV

Inter-Session Network Coding: Scalar and vector linear network coding, Fractional coding problem formulation, Insufficiency of linear network coding, Information theoretic approaches: Multiple unicast networks; Constructive approaches: Pairwise XOR coding in wireline networks, XOR coding in wireless networks.

Network Coding in Lossy Networks: Random linear network coding, Coding theorems: Unicast connections, Multicast connections, Error exponents for Poisson traffic with i.i.d. losses.

Subgraph Selection: Flow-based approaches: Intra-session coding, Computation-constrained coding, Inter-session coding; Queue-Length-Based approaches: Intra-session network coding for multicast sessions, Inter-session coding.

UNIT - V

Multiple Sources Network Coding:

Superposition coding and max-flow bound; Network Codes for Acyclic Networks: Achievable information rate region, Inner bound R_{in}, Outer bound R_{out}, R_{LP} – An explicit outer bound.

Security against adversarial Errors: Error correction: Error Correcting bounds for centralized network coding, Distributed random network coding and polynomial-complexity error correction; Detection of adversarial errors: Model and problem formulation, Detection probability.

TEXT BOOKS:

1. Raymond W. Yeung, Shuo-Yen Robert Li, Ning Cai, Zhen Zhang, “Network Coding Theory”, now publishers Inc, 2006, ISBN: 1-933019-24-7.
2. Christina Fragouli, Emina Soljanin, “Network Coding Fundamentals”, now publishers Inc, 2007, ISBN: 978-1-60198-032-8.

REFERENCES:

1. Tracey Ho, Desmond Lun, “Network Coding: An Introduction”, Cambridge University Press, 2008, ISBN: 978-0-521-87310-9.
2. Muriel Medard, Alex Sprintson, “Network Coding: Fundamentals and Applications”, 1st Edition, 2012, Academic Press, Elsevier, ISBN: 978-0-12-380918-6.

ADVANCED WIRELESS NETWORKS (Professional Elective - II)

M.Tech CNIS/CN/CYS I Year I Sem.

L	T	P	C
3	0	0	3

Pre-Requisites: Computer Networks

Course Objectives:

1. The students should get familiar with the wireless/mobile market and the future needs and challenges.
2. To get familiar with key concepts of wireless networks, standards, technologies and their basic Operations.
3. To learn how to design and analyze various medium access.
4. To learn how to evaluate MAC and network protocols using network simulation software tools.
5. The students should get familiar with the wireless/mobile market and the future needs and challenges.

Course Outcomes: After completion of course, students would be able to:

1. Demonstrate advanced knowledge of networking and wireless networking and understand various types of wireless networks, standards, operations and use cases.
2. Be able to design WLAN, WPAN, WWAN, Cellular based upon underlying propagation and performance analysis.
3. Demonstrate knowledge of protocols used in wireless networks and learn simulating wireless networks.
4. Design wireless networks exploring trade-offs between wireline and wireless links.
5. Develop mobile applications to solve some of the real-world problems.

UNIT - I

Introduction:

Wireless Networking Trends, Key Wireless Physical Layer Concepts, Multiple Access Technologies - CDMA, FDMA, TDMA, Spread Spectrum technologies, Frequency reuse, Radio Propagation and Modelling, Challenges in Mobile Computing: Resource poorness, Bandwidth, energy etc.

UNIT – II

Wireless Local Area Networks:

IEEE 802.11 Wireless LANs Physical & MAC layer, 802.11 MAC Modes (DCF& PCF) IEEE 802.11 standards, Architecture & protocols, Infrastructure vs. Adhoc Modes, Hidden Node & Exposed Terminal Problem, Problems, Fading Effects in Indoor and outdoor WLANs, WLAN Deployment issues

UNIT - III

Wireless Cellular Networks:

1G and 2G, 2.5G, 3G, and 4G, Mobile IPv4, Mobile IPv6, TCP over Wireless Networks, Cellular architecture, Frequency reuse, Channel assignment strategies, Handoff strategies

UNIT - IV

WiMAX (Physical layer, Media access control, Mobility and Networking), IEEE802.22 Wireless Regional Area Networks, IEEE 802.21 Media Independent Handover Overview

Wireless Sensor Networks:

Introduction to Wireless Sensors, Application, Physical, MAC layer and Network Layer, Power Management.

UNIT - V

Security:

Security in wireless Networks Vulnerabilities, Security techniques, Wi-Fi Security, DoS in wireless communication.

Advanced Topics

Wireless PANs, Bluetooth AND Zigbee, Introduction to Vehicular Adhoc Networks

TEXT BOOKS:

1. Schiller J., Mobile Communications, Addison Wesley 2000
2. Stallings W., Wireless Communications and Networks, Pearson Education 2005

REFERENCES:

1. Stojmenic Ivan, Handbook of Wireless Networks and Mobile Computing, John Wiley and Sons Inc 2002
2. Yi Bing Lin and Imrich Chlamtac, Wireless and Mobile Network Architectures, John Wiley and Sons Inc 2000
3. Pandya Raj, Mobile and Personal Communications Systems and Services, PHI 200

DIGITAL FORENSICS (Professional Elective - II)

M.Tech CNIS/CN/CYS I Year I Sem.

L	T	P	C
3	0	0	3

Pre-Requisites: Cybercrime and Information Warfare, Computer Networks

Course Objectives:

1. provides an in-depth study of the rapidly changing and fascinating field of computer forensics.
2. Combines both the technical expertise and the knowledge required to investigate, detect and prevent digital crimes.
3. Knowledge on digital forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation, e-discovery tools
4. E-evidence collection and preservation, investigating operating systems and file systems, network forensics, art of steganography and mobile device forensics

Course Outcomes: On completion of the course the student should be able to

1. Understand relevant legislation and codes of ethics.
2. Computer forensics and digital detective and various processes, policies and procedures.
3. E-discovery, guidelines and standards, E-evidence, tools and environment.
4. Email and web forensics and network forensics.

UNIT - I

Digital Forensics Science: Forensics science, computer forensics, and digital forensics.

Computer Crime: Criminalistics as it relates to the investigative process, analysis of cyber criminalistics area, holistic approach to cyber-forensics

UNIT - II

Cyber Crime Scene Analysis:

Discuss the various court orders etc., methods to search and seizure electronic evidence, retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation.

UNIT - III

Evidence Management & Presentation:

Create and manage shared folders using operating system, importance of the forensic mindset, define the workload of law enforcement, Explain what the normal case would look like, Define who should be notified of a crime, parts of gathering evidence, Define and apply probable cause.

UNIT - IV

Computer Forensics: Prepare a case, Begin an investigation, Understand computer forensics workstations and software, Conduct an investigation, Complete a case, Critique a case,

Network Forensics: open-source security tools for network forensic analysis, requirements for preservation of network data.

UNIT - V

Mobile Forensics: mobile forensics techniques, mobile forensics tools.

Legal Aspects of Digital Forensics: IT Act 2000, amendment of IT Act 2008.

Recent trends in mobile forensic technique and methods to search and seizure electronic evidence

TEXT BOOKS:

1. John Sammons, The Basics of Digital Forensics, Elsevier
2. John Vacca, Computer Forensics: Computer Crime Scene Investigation, Laxmi Publications

REFERENCES:

1. William Oettinger, Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence, Packt Publishing; 1st edition (30 April 2020), ISBN: 1838648178.
2. Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar, Cybercrime and Digital Forensics: An Introduction, Routledge.

ADVANCED DATA STRUCTURES LAB (Lab- I)

M.Tech CNIS/CN/CYS I Year I Sem.

L	T	P	C
0	0	4	2

Prerequisites:

1. A course on Computer Programming & Data Structures

Course Objectives:

1. Introduces the basic concepts of Abstract Data Types.
2. Reviews basic data structures such as stacks and queues.
3. Introduces a variety of data structures such as hash tables, search trees, tries, heaps, graphs, and B-trees.
4. Introduces sorting and pattern matching algorithms.

Course Outcomes:

1. Ability to select the data structures that efficiently model the information in a problem.
2. Ability to assess efficiency trade-offs among different data structure implementations or combinations.
3. Implement and know the application of algorithms for sorting and pattern matching.
4. Design programs using a variety of data structures, including hash tables, binary and general tree structures, search trees, tries, heaps, graphs, and B-trees.

List of Programs

1. Write a program to perform the following operations:
   a) Insert an element into a binary search tree.
   b) Delete an element from a binary search tree.
   c) Search for a key element in a binary search tree.

2. Write a program for implementing the following sorting methods:
   a) Merge sort b) Heap sort c) Quick sort

3. Write a program to perform the following operations:
   a) Insert an element into a B- tree.
   b) Delete an element from a B- tree.
   c) Search for a key element in a B- tree.

4. Write a program to perform the following operations:
   a) Insert an element into a Min-Max heap
   b) Delete an element from a Min-Max heap
   c) Search for a key element in a Min-Max heap

5. Write a program to perform the following operations:
   a) Insert an element into a Lefiist tree
   b) Delete an element from a Leftist tree
   c) Search for a key element in a Leftist tree

6. Write a program to perform the following operations:
   a) Insert an element into a binomial heap
   b) Delete an element from a binomial heap.
   c) Search for a key element in a binomial heap

7. Write a program to perform the following operations:

a) Insert an element into a AVL tree.
b) Delete an element from a AVL search tree.
c) Search for a key element in a AVL search tree.

8. Write a program to perform the following operations:
a) Insert an element into a Red-Black tree.
b) Delete an element from a Red-Black tree.
c) Search for a key element in a Red-Black tree.

9. Write a program to implement all the functions of a dictionary using hashing.

10. Write a program for implementing Knuth-Morris-Pratt pattern matching algorithm.

11. Write a program for implementing Brute Force pattern matching algorithm.

12. Write a program for implementing Boyer pattern matching algorithm.

TEXT BOOKS:

1. Fundamentals of Data structures in C, E. Horowitz, S. Sahni and Susan Anderson Freed, 2nd Edition, Universities Press
2. Data Structures Using C – A.S. Tanenbaum, Y. Langsam, and M.J. Augenstein, PHI/Pearson education.
3. Introduction to Data Structures in C, Ashok Kamthane, 1st Edition, Pearson.

REFERENCES:

1. The C Programming Language, B.W. Kernighan, Dennis M. Ritchie, PHI/Pearson Education
2. C Programming with problem solving, J.A. Jones & K. Harrow, Dreamtech Press
3. Data structures: A Pseudocode Approach with C, R.F. Gilberg And B.A. Forouzan, 2nd Edition, Cengage Learning

INFORMATION SECURITY LAB (Lab- II)

M.Tech CNIS/CN/CYS I Year I Sem.

L	T	P	C
0	0	4	2

Course Objectives:

1. To implement the cryptographic algorithms.
2. To implement the security algorithms.
3. To implement cryptographic, digital signatures algorithms.

Course Outcomes:

1. Demonstrate the knowledge of cryptography, network security concepts and applications.
2. Ability to apply security principles in system design.
3. Ability to identify and investigate vulnerabilities and security threats and mechanisms to counter them

List of Experiments:

1. Implementation of symmetric cipher algorithm (AES and RC4)
2. Random number generation using a subset of digits and alphabets.
3. Implementation of RSA based signature system
4. Implementation of Subset sum
5. Authenticating the given signature using the MD5 hash algorithm.
6. Implementation of Diffie-Hellman algorithm
7. Implementation of the ELGAMAL cryptosystem.
8. Implementation of Goldwasser-Micali probabilistic public key system
9. Implementation of Rabin Cryptosystem. (Optional).
10. Implementation of Kerberos cryptosystem
11. Firewall implementation and testing.
12. Implementation of a trusted secure web transaction.
13. Cryptographic Libraries-Sun JCE/OpenSSL/Bouncy Castle JCE.
14. Digital Certificates and Hybrid (ASSY/SY) encryption, PKI.
15. Message Authentication Codes.
16. Elliptic Curve cryptosystems (Optional)
17. PKCS Standards (PKCS1, 5, 11, 12), Cipher modes.

TEXT BOOK:

1. Cryptography and Network Security (principles and approaches) by William Stallings Pearson Education, 4th Edition.

REFERENCES:

1. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education.
2. Principles of Information Security, Whitman, Thomson.

VULNERABILITY ASSESSMENT & PENETRATION TESTING LAB (Lab- II)

M.Tech CNIS/CN/CYS I Year I Sem.

L	T	P	C
0	0	4	2

Course Objectives: This lab session focuses on training the students in

1. Penetration Testing methodologies
2. Monitoring the network traffic and
3. To understand the host and services discovery

Course Outcomes:

1. Design for monitoring network traffic
2. Perform different penetration testing methods
3. Design different types of vulnerabilities scanning
4. Understand web application assessment

List of Experiments:

1. Monitoring Network Traffic
2. Host & Services Discovery using Nmap
3. Vulnerability Scanning using OpenVAS
4. Internal Penetration Testing
   a. Mapping
   b. Scanning
   c. Gaining access through CVE's
   d. Sniffing POP3/FTP/Telnet Passwords
   e. ARP Poisoning
   f. DNS Poisoning
5. External Penetration Testing
   a. Evaluating external Infrastructure
   b. Creating topological map & identifying IP address of target
   c. Lookup domain registry for IP information
   d. Examining use of IPV6 at remote location

6. Different types of vulnerability scanning
7. Vulnerability scanning with Nessus
8. Web application assessment with nikto & burp suite

TEXT BOOKS:

1. Gray Hat Hacking-The Ethical Hackers Handbook, Allen Harper, Stephen Sims, Michael Baucom, 3rd Edition, Tata Mc Graw-Hill.
2. The Web Application Hacker's Handbook-Discovering and Exploiting Security flaws, Dafydd Suttard, Marcus pinto, 1st Edition, Wiley Publishing.

REFERENCES:

1. Penetration Testing: Hands-on Introduction to Hacking, Georgia Weidman, 1st Edition, No Starch Press.
2. The Pen Tester Blueprint-Starting a Career as an Ethical Hacker, L. Wylie, Kim Crawly, 1st Edition, Wiley Publications.

MOBILE APPLICATION SECURITY LAB (Lab- II)

M.Tech CNIS/CN/CYS I Year I Sem.

L	T	P	C
0	0	4	2

Course Objectives: This course provides a thorough understanding of mobile platforms, including attack surfaces, risk landscape & more.

Course Outcomes:

1. Understand common mobile application security vulnerabilities
2. Understand and analyze the apks using different tools
3. understand and implement authentication services.

List of Experiments

1. Use the following tools to analyze an apk to detect for any existence of vulnerabilities
    a. QARK
    b. DEVKNOX
    c. OWASP
    d. DROZER
2. Implement Authentication: Single Sign-on
3. Implement Authentication: Two Factor Authentication
4. Demonstrate how to Detect and Remove Malware From Android Phone
5. Demonstrate Remote Lock or Wipe

TEXT BOOKS:

1. Mobile Application Security, Himanshu Dwivedi, Chris Clark, David Thiel, TATA McGraw-Hill.

REFERENCES:

1. Mobile and Wireless Network Security and Privacy, Kami S. Makki, et al, Springer.
2. Android Security Attacks Defenses, Abhishek Dubey, CRC Press

RESEARCH METHODOLOGY & IPR

M.Tech CNIS/CN/CYS I Year I Sem.

L	T	P	C
2	0	0	2

Course Objectives:

1. To understand the research problem
2. To know the literature studies, plagiarism and ethics
3. To get the knowledge about technical writing
4. To analyze the nature of intellectual property rights and new developments
5. To know the patent rights

Course Outcomes: At the end of this course, students will be able to

1. Understand research problem formulation.
2. Analyze research related information
3. Follow research ethics
4. Understand that today's world is controlled by Computer, Information Technology, but tomorrow world will be ruled by ideas, concept, and creativity.
5. Understanding that when IPR would take such important place in growth of individuals & nation, it is needless to emphasis the need of information about Intellectual Property Right to be promoted among students in general & engineering in particular.
6. Understand that IPR protection provides an incentive to inventors for further research work and investment in R & D, which leads to creation of new and better products, and in turn brings about, economic growth and social benefits.

UNIT- I:

Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem. Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations

UNIT- II:

Effective literature studies approaches, analysis, Plagiarism, Research ethics

UNIT- III:

Effective technical writing, how to write report, Paper Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee

UNIT- IV:

Nature of Intellectual Property: Patents, Designs, Trade and Copyright. Process of Patenting and Development: technological research, innovation, patenting, development. International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, Patenting under PCT.

UNIT- V:

Patent Rights: Scope of Patent Rights. Licensing and transfer of technology. Patent information and databases. Geographical Indications. New Developments in IPR: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Software etc. Traditional knowledge Case Studies, IPR and IITs.

TEXT BOOKS:

1. Stuart Melville and Wayne Goddard, "Research methodology: an introduction for science & engineering students'"

2. Wayne Goddard and Stuart Melville, “Research Methodology: An Introduction”

REFERENCE BOOKS:

1. Ranjit Kumar, 2nd Edition, “Research Methodology: A Step by Step Guide for beginners”
2. Halbert, “Resisting Intellectual Property”, Taylor & Francis Ltd ,2007.
3. Mayall, “Industrial Design”, McGraw Hill, 1992.
4. Niebel, “Product Design”, McGraw Hill, 1974.
5. Asimov, “Introduction to Design”, Prentice Hall, 1962.
6. Robert P. Merges, Peter S. Menell, Mark A. Lemley, “Intellectual Property in New Technological Age”, 2016.
7. T. Ramappa, “Intellectual Property Rights Under WTO”, S. Chand, 2008

DISTRIBUTED SYSTEMS (PC - III)

M.Tech CNIS/CN/CYS I Year II Sem.

L	T	P	C
3	0	0	3

Prerequisites: A course on “Operating Systems”.

Course Objectives: This course provides an insight into Distributed systems.
Topics include- Peer to Peer Systems, Transactions and Concurrency control, Security and Distributed shared memory

Course Outcomes:

1. Ability to understand Distributed Transactions and Concurrency control.
2. Ability to understand Security issues.
3. Understanding Distributed shared memory.
4. Analyze communication methods in distributed systems

UNIT - I

Characterization of Distributed Systems-Introduction, Examples of Distributed systems, Resource sharing and web, challenges, System models-Introduction, Architectural and Fundamental models, Networking and Internetworking, Interprocess Communication,
Distributed objects and Remote Invocation-Introduction, Communication between distributed objects, RPC, Events and notifications, Case study-Java RMI.

UNIT - II

Operating System Support- Introduction, OS layer, Protection, Processes and Threads, Communication and Invocation, Operating system architecture, Distributed File Systems-Introduction, File Service architecture, case study- SUN network file systems.
Name Services-Introduction; Name Services and the Domain Name System, Case study of the Global Name Service, Case study of the X.500 Directory Service.

UNIT - III

Peer to Peer Systems–Introduction, Napster and its legacy, Peer to Peer middleware, Routing overlays, Overlay case studies-Pastry, Tapestry, Application case studies-Squirrel, OceanStore.
Time and Global States-Introduction, Clocks, events and Process states, Synchronizing physical clocks, logical time and logical clocks, global states, distributed debugging.
Coordination and Agreement-Introduction, Distributed mutual exclusion, Elections, Multicast communication, consensus and related problems.

UNIT - IV

Transactions and Concurrency control-Introduction, Transactions, Nested Transactions, Locks, Optimistic concurrency control, Timestamp ordering, Comparison of methods for concurrency control. Distributed Transactions-Introduction, Flat and Nested Distributed Transactions, Atomic commit protocols, Concurrency control in distributed transactions, Distributed deadlocks, Transaction recovery, Replication-Introduction, System model and group communication, Fault tolerant services, Transactions with replicated data.

UNIT - V

Security-Introduction, Overview of Security techniques, Cryptographic algorithms, Digital signatures, Case studies-Kerberos, TLS, 802.11 WiFi.
Distributed shared memory, Design and Implementation issues, Sequential consistency and Ivy case study, Release consistency and Munin case study, Other consistency models, CORBA case study-Introduction, CORBA RMI, CORBA Services.

TEXT BOOKS:

1. Distributed Systems Concepts and Design, G Coulouris, J Dollimore and T Kindberg, Fourth Edition, Pearson Education.
2. Distributed Systems, S. Ghosh, Chapman & Hall/CRC, Taylor & Francis Group, 2010.

REFERENCES:

1. Distributed Computing, S. Mahajan and S. Shah, Oxford University Press.
2. Distributed Operating Systems Concepts and Design, Pradeep K.Sinha, PHI.
3. Advanced Concepts in Operating Systems, M Singhal, N G Shivarathri, TMH.
4. Reliable Distributed Systems, K. P. Birman, Springer.
5. Distributed Systems – Principles and Paradigms, A.S. Tanenbaum and M.V. Steen, Pearson Education.
6. Distributed Operating Systems and Algorithm Analysis, R. Chow, T. Johnson, Pearson.
7. Distributed Operating Systems, A. S. Tanenbaum, Pearson education.
8. Distributed Computing, Principles, Algorithms and Systems, Ajay D. Kshemakalyani and Mukesh Singhal, Cambridge, rp 2010.

WEB & DATABASE SECURITY (PC - IV)

M.Tech CNIS/CN/CYS I Year II Sem.

L	T	P	C
3	0	0	3

Course Objectives:

1. Give an Overview of information security
2. Give an overview of Access control of relational databases

Course Outcomes: Students should be able to

1. Understand the Web architecture and applications
2. Understand client side and server side programming
3. Understand how common mistakes can be bypassed and exploit the application
4. Identify common application vulnerabilities

UNIT - I

The Web Security,The Web Security Problem ,Risk Analysis and Best Practices
Cryptography and the Web: Cryptography and Web Security, Working Cryptographic Systems and Protocols, Legal Restrictions on Cryptography, Digital Identification

UNIT - II

The Web's War on Your Privacy, Privacy-Protecting Techniques, Backups and Antitheft, Web Server Security, Physical Security for Servers, Host Security for Servers, Securing Web Applications

UNIT - III

Database Security: Recent Advances in Access Control, Access Control Models for XML, Database Issues in Trust Management and Trust Negotiation, Security in Data Warehouses and OLAP Systems

UNIT - IV

Security Re-engineering for Databases: Concepts and Techniques, Database Watermarking for Copyright Protection, Trustworthy Records Retention, Damage Quarantine and Recovery in Data Processing Systems, Hippocratic Databases: Current Capabilities and

UNIT - V

Future Trends Privacy in Database Publishing: A Bayesian Perspective, Privacy-enhanced Location-based Access Control, Efficiently Enforcing the Security and Privacy Policies in a Mobile Environment

TEXT BOOK:

1. Web Security, Privacy and Commerce Simson Garfinkel, Gene Spafford, O'Reilly.
2. Handbook on Database security applications and trends Michael Gertz, Sushil Jajodia

REFERENCES:

1. Andrew Hoffman, Web Application Security: Exploitation and Countermeasures for Modern Web Applications, O'reilly
2. Jonathan LeBlanc Tim Messerschmidt, Identity and Data Security for Web Development - Best Practices, O'reilly
3. McDonald Malcolm, Web Security for Developers, No Starch Press, US

INTRUSION DETECTION & PREVENTION SYSTEMS (Professional Elective - III)

M.Tech CNIS/CN/CYS I Year II Sem.

L	T	P	C
3	0	0	3

Course Objectives:

1. To understand about the intruders.
2. To know the intrusion detection and prevention policies

Course Outcomes:

1. Understand intrusion detection systems and prevention basics
2. Analyze architecture and implementation of intrusion detection systems.
3. Analyze various applications and tools of Intrusion detection
4. Illustrate Legal Issues and Organizations Standards.

UNIT- I

Introduction: Understanding Intrusion Detection – Intrusion detection and prevention basics – IDS and IPS analysis schemes, Attacks, Detection approaches –Misuse detection – anamoly detection – specification-based detection – hybrid detection THEORETICAL FOUNDATIONS OF DETECTION: Taxonomy of anomaly detection system – fuzzy logic – Bayes theory – Artificial Neural networks – Support vector machine – Evolutionary computation – Association rules – Clustering

UNIT- II

Architecture and Implementation: Centralized – Distributed – Cooperative Intrusion Detection - Tiered architecture

UNIT- III

Justifying Intrusion Detection: Intrusion detection in security – Threat Briefing – Quantifying risk – Return on Investment (ROI)

UNIT- IV

Applications and Tools: Tool Selection and Acquisition Process - Bro Intrusion Detection – Prelude Intrusion Detection - Cisco Security IDS - Snorts Intrusion Detection – NFR security

UNIT- V

Legal Issues and Organizations Standards: Law Enforcement / Criminal Prosecutions – Standard of Due Care – Evidentiary Issues, Organizations and Standardizations.

TEXT BOOKS:

1. Ali A. Ghorbani, Wei Lu, “Network Intrusion Detection and Prevention: Concepts and Techniques”, Springer, 2010.
2. Carl Enrolf, Eugene Schultz, Jim Mellander, “Intrusion detection and Prevention”, McGraw Hill, 2004

REFERENCES:

1. Paul E. Proctor, “The Practical Intrusion Detection Handbook “, Prentice Hall, 2001.
2. Ankit Fadia and Mnu Zacharia, “Intrusiion Alert”, Vikas Publishing house Pvt., Ltd, 2007.
3. Earl Carter, Jonathan Hogue, “Intrusion Prevention Fundamentals”, Pearson Education, 2006.

CLOUD SECURITY (Professional Elective - III)

M.Tech CNIS/CN/CYS I Year II Sem.

L	T	P	C
3	0	0	3

Pre-requisites: Computer Networks, Cryptography and Network Security, Cloud Computing.

Course Objectives:

1. To understand the fundamentals concepts of cloud computing.
2. To understand the cloud security and privacy issues.
3. To understand the Threat Model and Cloud Attacks
4. To understand the Data Security and Storage
5. To analyze Security Management in the Cloud.

Course Outcome:

1. Ability to acquire the knowledge on fundamentals concepts of cloud computing.
2. Able to distinguish the various cloud security and privacy issues.
3. Able to analyze the various threats and Attack tools
4. Able to understand the Data Security and Storage
5. Able to analyze the Security Management in the Cloud.

UNIT - I

Overview of Cloud Computing: Introduction, Definitions and Characteristics, Cloud Service Models, Cloud Deployment Models, Cloud Service Platforms, Challenges Ahead.

Introduction to Cloud Security: Introduction, Cloud Security Concepts, CSA Cloud Reference Model, NIST Cloud Reference Model, NIST Cloud Reference Model.

UNIT - II

Cloud Security and Privacy Issues: Introduction, Cloud Security Goals/Concepts, Cloud Security Issues, Security Requirements for Privacy, Privacy Issues in Cloud.

Infrastructure Security: The Network Level, the Host Level,the Application Level, SaaS Application Security, PaaS Application Security, IaaS Application Security.

UNIT - III

Threat Model and Cloud Attacks: Introduction, Threat Model- Type of attack entities, Attack surfaces with attack scenarios, A Taxonomy of Attacks, Attack Tools-Network-level attack tools, VM-level attack tools, VMM attack tools, Security Tools, VMM security tools.

UNIT - IV

Information Security Basic Concepts, an Example of a Security Attack, Cloud Software Security Requirements, Rising Security Threats.

Data Security and Storage: Aspects of Data Security, Data Security Mitigation, Provider Data and Its Security.

UNIT - V

Evolution of Security Considerations, Security Concerns of Cloud Operating Models, Identity Authentication, Secure Transmissions, Secure Storage and Computation, Security Using Encryption Keys, Challenges of Using Standard Security Algorithms, Variations and Special Cases for Security Issues with Cloud Computing, Side Channel Security Attacks in the Cloud

Security Management in the Cloud- Security Management Standards, Availability Management, Access Control, Security Vulnerability, Patch, and Configuration Management.

TEXT BOOKS:

1. Cloud Security Attacks, Techniques, Tools, and Challenges by Preeti Mishra, Emmanuel S Pilli, Jaipur R C Joshi Graphic Era, 1st Edition published 2022 by CRC press.
2. Cloud Computing with Security Concepts and Practices Second Edition by Naresh Kumar Sehgal Pramod Chandra, P. Bhatt John M. Acken, 2nd Edition Springer nature Switzerland AG 2020.
3. Cloud Security and Privacy by Tim Mather, Subra Kumaraswamy, and Shahed Lati First Edition, September 2019.

REFERENCES:

1. Essentials of Cloud Computing by K. Chandrasekaran Special Indian Edition CRC press.
2. Cloud Computing Principles and Paradigms by Rajkumar Buyya, John Wiley.

BLOCKCHAIN TECHNOLOGY (Professional Elective - III)

M.Tech CNIS/CN/CYS I Year II Sem.

L	T	P	C
3	0	0	3

Pre-requisites:

1. Knowledge in information security and applied cryptography.
2. Knowledge in distributed databases.

Course Objectives:

1. To learn the fundamentals of BlockChain and various types of block chain and consensus mechanism.
2. To understand public block chain system, Private block chain system and consortium blockchain.
3. Able to know the security issues of blockchain technology.

Course Outcomes: Able to work in the field of block chain technologies.

UNIT-I

Fundamentals of Blockchain: Introduction, Origin of Blockchain, Blockchain Solution, Components of Blockchain, Block in a Blockchain,The Technology and the Future. Blockchain Types and Consensus Mechanism: Introduction, Decentralization and Distribution, Types of Blockchain, Consensus Protocol.

Cryptocurrency – Bitcoin, Altcoin and Token: Introduction, Bitcoin and the Cryptocurrency, Cryptocurrency Basics, Types of Cryptocurrencies, Cryptocurrency Usage.

UNIT-II

Public Blockchain System: Introduction, Public Blockchain, Popular Public Blockchains, The Bitcoin Blockchain, Ethereum Blockchain.

Smart Contracts: Introduction, Smart Contract, Characteristics of a Smart Contract, Types of Smart Contracts, Types of Oracles, Smart Contracts in Ethereum, Smart Contracts in Industry.

UNIT-III

Private Blockchain System: Introduction, Key Characteristics of Private Blockchain, Why We Need Private Blockchain, Private Blockchain Examples, Private Blockchain and Open Source, E-commerce Site Example, Various Commands (Instructions) in E-commerce Blockchain, Smart Contract in Private Environment, State Machine, Different Algorithms of Permissioned Blockchain, Byzantine Fault, Multichain.

Consortium Blockchain: Introduction, Key Characteristics of Consortium Blockchain, Why We Need Consortium Blockchain, Hyperledger Platform, Overview of Ripple, Overview of Corda. Initial Coin Offering: Introduction, Blockchain Fundraising Methods, Launching an ICO, Investing in an ICO, Pros and Cons of Initial Coin Offering, Successful Initial Coin Offerings, Evolution of ICO, ICO Platforms.

UNIT-IV

Security in Blockchain: Introduction, Security Aspects in Bitcoin, Security and Privacy Challenges of Blockchain in General, Performance and Scalability, Identity Management and Authentication, Regulatory Compliance and Assurance, Safeguarding Blockchain Smart Contract (DApp), Security Aspects in Hyperledger Fabric.

Applications of Blockchain: Introduction, Blockchain in Banking and Finance, Blockchain in Education, Blockchain in Energy, Blockchain in Healthcare, Blockchain in Real-estate, Blockchain in Supply Chain, The Blockchain and IoT. Limitations and Challenges of Blockchain.

UNIT-V

Blockchain Case Studies: Case Study 1 – Retail, Case Study 2 – Banking and Financial Services, Case Study 3 – Healthcare, Case Study 4 – Energy and Utilities. Blockchain Platform using Python: Introduction, Learn How to Use Python Online Editor, Basic Programming Using Python, Python Packages for Blockchain.

Blockchain platform using Hyperledger Fabric: Introduction, Components of Hyperledger Fabric Network, Chain codes from Developer.ibm.com, Blockchain Application Using Fabric Java SDK.

TEXT BOOKS:

1. "Block chain Technology", Chandramouli Subramanian, Asha A.George, Abhilash K A and Meena Karthikeyan, Universities Press.

REFERENCES:

1. Blockchain Blueprint for Economy, Melanie Swan, SPD O'reilly.
2. Blockchain for Business, Jai Singh Arun, Jerry Cuomo, Nitin Gaur, Pearson Addition Wesley.

DIGITAL PAYMENT SYSTEMS (Professional Elective - IV)

M.Tech CNIS/CN/CYS I Year II Sem.

L	T	P	C
3	0	0	3

Course Objectives: The aim of the course:

1. Discuss the players and processes involved in e-payments
2. Discuss the different categories and potential uses of smart cards

Course Outcomes:

1. Understand the shifts that are occurring with regard to digital payments.
2. Acquire a comprehensive understanding of different tasks associated in usage of digital payment systems.
3. Understand risks involved in e-payments and their counter-measures to provide secure transactions.
4. Understand and analyze chip card technology for digital payment systems.

UNIT - I

Introduction, Magnetic stripe debit and Credit cards, Chip Migration with EMV™, Remote debit and credit with EMV™

Payment Card Processing

Roles involved in payment card processing, payment card brands, Credit and debit payment cards, Focusing on the magnetic stripe card, Threats and security protections, Processing at the point of service, Payment network and interchange message, On-line authorization, Clearing and Settlement.

UNIT - II

A business case for chip migration, An overview of the chip card technology, proprietary payment application, interoperable payment application, EMV™ data elements, EMV™ file system, EMV™ application selection.

SMS Payments, USSD Payments, UPI Payments, Mobile Wallets, Bharat Bill Payments, NEFT, IMPS, QR Code, Merchants Payments, Internet Banking & Payments. ATM Payments, Interoperable Payments.

UNIT - III

Certification mechanism and algorithm, Public key certificate for RSA scheme, Entities and certifiers, Entity public key remainder, EMV™ certification chain, Issuing EMV™ public key certificates, Verifying EMV™ public key certificates, Issuing signed static application data, Verifying the signed static application data.

UNIT - IV

Overview of the EMV™ debit/credit transaction, Initiate application processing, Read application data, Off-line data authentication, Processing restrictions, Cardholder Verification, Terminal risk management, Terminal action analysis, On-line processing and issuer authentication.

UNIT - V

EMV™ regulatory framework, Deriving ICC specifications by issuers, Selection criteria of the ICC architecture, Multiplication ICC, Issuer's business case, adaptive initiate application processing, Design criteria for CAM selection, Design criteria for CVM, Processing restrictions, Card risk management.

TEXT BOOKS:

1. Cristian Radu, Artech House, Implementing Electronic Card Payment Systems, Computer Security Series

REFERENCES:

1. Electronic Payment Systems for E-Commerce by Donal O'Mahony, Michael Peirce and Hitesh Tewari, Artech House, Computer Security Series
2. David A. Buchanan, James McCalman, High Performance Work Systems: The Digital Experience, Routledge
3. David A. Montague, Essentials of Online payment Security and Fraud Prevention, Wiley

USER AUTHENTICATION TECHNIQUES (Professional Elective - IV)

M.Tech CNIS/CN/CYS I Year II Sem.

L	T	P	C
3	0	0	3

Course Objectives: Knowledge on concept of authentication types, protocols, physical identification and various authentication algorithms

Course Outcomes:

1. Understand different types of authentication techniques
2. Understand text based and voice based authentication techniques
3. Understand significance of authentication algorithms and its standards
4. Apply various authentication protocols in multi-server environment and their representation

UNIT-I:

Definition of Authentication, Identification/verification, Stages and steps of authentication, Authentication Entity : User, Device and Application; Authentication attributes: Source, Location, Path, Time duration etc.; Authentication Types : Direct / Indirect, One Way / Mutual, On demand/ Periodic/ Dynamic/Continuous authentication, Assisted/Automatic; 3 Factors of authentication; Passwords, Generation of passwords of varied length and of mixed type, OTP, passwords generation using entity identity credentials; Secure capture, processing, storage, verification and retrieval of passwords;

UNIT -II:

Physical identification using smart cards, remote control device, proximity sensors, surveillance camera, authentication in Card present / Card Not Present transactions as ATM/ PoS Device, mobile phone, wearable devices and IoT device based authentication; single sign- on; Symmetric Key Generation, Key Establishment, Key Agreement Protocols;

UNIT - III:

Biometrics – photo, face, iris, retinal, handwriting, signature, fingerprint, palm print, hand geometry, voice – Text based and text independent voice authentication, style of talking, walking, writing, keystrokes, gait etc. multimodal biometrics.

UNIT - IV:

Matching algorithms, Patterns analysis, errors, performance measures, ROC Curve; Authentication Standards – International, UIDAI Standard. Kerberos, X.509 Authentication Service, Public Key Infrastructure, Scanners and Software; Web Authentication Methods: Http based, Token Based, OAuthand API.

UNIT - V:

User authentication protocols in multi-server environment, BAN Logic, Representation of authentication protocols using BAN Logic, Random Oracle Model, Scyther Tools, Proverif tool, Chebyshev Chaotic Map, Fuzzy Extractor, Fuzzy Extractor Map, Bloom Filter, LU Decomposition based User Authentication, Blockchain based authentication.

TEXT BOOKS:

1. Protocols for Authentication and Key Establishment, Colin Boyd and Anish Mathuria, springer, 2021
2. Guide to Biometrics, Ruud M.Bolle, Sharath Pankanti, Nalini K. Ratha, Andrew W. Senior, Jonathan H. Connell, Springer 2009.

REFERENCES:

1. Digital Image Processing using MATLAB, Rafael C. Gonzalez, Richard Eugene Woods, 2nd Edition, Tata McGraw-Hill Education 2010.
2. Biometric System and Data Analysis: Design, Evaluation, and data Mining, Ted Dunstone and Neil Yager, Springer.
3. Biometrics Technologies and verification Systems, John Vacca, , Elsevier Inc. , 2007.
4. Pattern Classification, Richard O. Duda, David G.Stork,Peter E. Hart, Wiley 2007.

DATA ANALYTICS FOR FRAUD DETECTION (Professional Elective - IV)

M.Tech CNIS/CN/CYS I Year II Sem.

L	T	P	C
3	0	0	3

Course Objectives:

1. Discuss the overall process of how data analytics is applied
2. Discuss how data analytics can be used to better address and identify risks
3. Help mitigate risks from fraud and waste for our clients and organizations

Course Outcomes:

1. Formulate reasons for using data analysis to detect fraud.
2. Explain characteristics and components of the data and assess its completeness.
3. Identify known fraud symptoms and use digital analysis to identify unknown fraud symptoms.
4. Automate the detection process.
5. Verify results and understand how to prosecute fraud

UNIT - I

Introduction: Defining Fraud, Anomalies versus, Fraud, Types of Fraud, Assess the Risk of Fraud, Fraud Detection, Recognizing Fraud, Data Mining versus Data Analysis and Analytics, Data Analytical Software, Anomalies versus Fraud within Data, Fraudulent Data Inclusions and Deletions

UNIT - II

The Data Analysis Cycle, Evaluation and Analysis, Obtaining Data Files, Performing the Audit, File Format Types, Preparation for Data Analysis, Arranging and Organizing Data,
Statistics and Sampling, Descriptive Statistics, Inferential Statistics

UNIT - III

Data Analytical Tests: Benford's Law, Number Duplication Test, Z-Score, Relative Size Factor Test, Same-Same-Same Test, Same-Same-Different Test

UNIT - IV

Advanced Data Analytical Tests
Correlation, Trend Analysis, GEL-1 and GEL-2, Skimming and Cash Larceny, Billing schemes: and Data Familiarization, Benford's Law Tests, Relative Size Factor Test, Match Employee Address to Supplier data

UNIT - V

Payroll Fraud, Expense Reimbursement Schemes, Register disbursement schemes

TEXT BOOK:

1. Fraud and Fraud Detection: A Data Analytics Approach by Sunder Gee, Wiley

REFERENCES:

1. Blokdyk Gerardus, Data analysis techniques for fraud detection, Createspace Independent Publishing Platform
2. Leonard W. Vona, Fraud Data Analytics Methodology: The Fraud Scenario Approach to Uncovering Fraud in Core Business Systems, Wiley

WEB & DATABASE SECURITY LAB (Lab - III)

M.Tech CNIS/CN/CYS I Year II Sem.

L	T	P	C
0	0	4	2

Pre-requisites: Database Management Systems, Practical exposure on Commercial Database Management Systems, Web Security,

Course Outcomes: At the end of the course the student will be able to:

1. Design of access control methods for secure web & database application development
2. Analyse and Classify the vulnerabilities in the Web and Database applications.
3. Design & implementation various methods for web & database intrusion detection.
4. Design and Implementation security audit methods.

List of Experiments:

1. Creation and manipulation of database using SQL scripts and graphical interfaces.
2. Implementing DAC: Implementation of database security policies using DAC in oracle 10g/SQL server
3. Implementing of MAC to ensure confidentiality and control information flow using either Oracle 10g or SQL server. This provides exposure to understand the concepts of MAC and Trojan hose
4. Implementation of Virtual Private Database using View using Oracle 10g or SQL server
5. Design a method to simulate the HTML injections and cross-site scripting (XSS) to exploit the attackers.
6. Determine HTML injection bugs and possible measures to prevent HTML injection exploits.
7. Implement Secure coding for buffer flow heap attacks.
8. Implementation of Design methods to break authentication schemes
9. Implementation of methods for abusing Design Deficiencies against web sites

INTRUSION DETECTION & PREVENTION SYSTEMS LAB (Professional Elective - III Lab)

M.Tech CNIS/CN/CYS I Year II Sem.

L	T	P	C
0	0	4	2

Course Objectives:

1. To understand about the intruders.
2. To know the intrusion detection and prevention policies

Course Outcomes:

1. Understand intrusion detection systems and prevention basics
2. Analyze architecture and implementation of intrusion detection systems.
3. Analyze various applications and tools of Intrusion detection
4. Illustrate Legal Issues and Organizations Standards.

List of Experiments

1. Configure and run open-source Snort and write Snort signatures
2. Configure and run open-source Zeek to provide a hybrid traffic analysis framework
3. Understand TCP/IP component layers to identify normal and abnormal traffic
4. Use open-source traffic analysis tools to identify signs of an intrusion
5. Comprehend the need to employ network forensics to investigate traffic to identify a possible intrusion
6. Use Wireshark to carve out suspicious file attachments
7. Write tcpdump filters to selectively examine a particular traffic trait
8. Craft packets with Scapy
9. Use the open-source network flow tool SiLK to find network behavior anomalies
10. Use your knowledge of network architecture and hardware to customize placement of IDS sensors and sniff traffic off the wire

CLOUD SECURITY LAB (Professional Elective - III Lab)

M.Tech CNIS/CN/CYS I Year II Sem.

L	T	P	C
0	0	4	2

Pre-requisites: Computer Networks, Cryptography and Network Security, Cloud Computing.

Course Objectives:

1. To understand the fundamentals concepts of cloud computing.
2. To understand the cloud security and privacy issues.
3. To understand the Threat Model and Cloud Attacks
4. To understand the Data Security and Storage
5. To analyze Security Management in the Cloud.

Course Outcomes:

1. Ability to acquire the knowledge on fundamentals concepts of cloud computing.
2. Able to distinguish the various cloud security and privacy issues.
3. Able to analyze the various threats and Attack tools
4. Able to understand the Data Security and Storage
5. Able to analyze the Security Management in the Cloud.

List of Experiments:

This lab mainly relies on Amazon Web Service (AWS), an IaaS cloud provider.
Students are required to register an AWS account.
Following task should be performed for different case studies

1. Infrastructure Security: *Network Architecture Design on Cloud: Design a secure network architecture on cloud:* Setup Virtual Private Cloud (VPC), Configure Subnet and Associate to VPC, Security Configuration on VPC
2. Instance Launching: Provide secure communication between Application server and Database server
3. Provisioning of Network level security, Host level security, Application level security in cloud
4. Illustrate Data security and Storage on cloud
5. Data privacy and security Issues, Jurisdictional issues raised by Data location
6. Identity & Access Management
7. Access Control
8. Trust, Reputation, Risk
9. Authentication in cloud computing, Client access in cloud, Cloud contracting Model, Commercial and business consideration

TEXT BOOKS:

1. Cloud Security Attacks, Techniques, Tools, and Challenges by Preeti Mishra, Emmanuel S Pilli, Jaipur R C Joshi Graphic Era, 1st Edition published 2022 by CRC press.
2. Cloud Computing with Security Concepts and Practices Second Edition by Naresh Kumar Sehgal Pramod Chandra, P. Bhatt John M. Acken,2nd Edition Springer nature Switzerland AG 2020.
3. Cloud Security and Privacy by Tim Mather, Subra Kumaraswamy, and Shahed Lati First Edition, September 2019.

REFERENCES:

1. Essentials of Cloud Computing by K. Chandrasekaran Special Indian Edition CRC press.
2. Cloud Computing Principles and Paradigms by Rajkumar Buyya, John Wiley.
3. https://www.nielit.gov.in/sites/default/files/cl.pdf
4. www.Sans.org

BLOCKCHAIN TECHNOLOGY LAB (Professional Elective - III Lab)

M.Tech CNIS/CN/CYS I Year II Sem.

L	T	P	C
0	0	4	2

Pre-requisites:

1. Knowledge in Basics of JavaScript /Java for Hyperledger Fabric.
2. Basics of Solidity for ETH.

Course Objectives:

1. To learn the basic blockchain applications.
2. To be familiar with the blockchain lab setup.

Course Outcomes: Able to work in the field of block chain technologies.

List of Experiments:

1) Setup Metamask in the System and Create a wallet in the Metamask with Test Network.

2) Create multiple accounts in Metamask and perform the balance transfer between the accounts and describe the transaction specifications.

3) Setup the Ganache Tool in the system.

4) Create a custom RPC network in Metamask and connect it with Ganache tool and transfer the ether between ganache accounts.

5) Write a smart contract using a solidity program to perform the balance transfer from contract to other accounts.

6) Write a solidity program to perform the exception handling.

7) Setup the Hyperledger Fabric Network with 2 Organizations 1 Peer Each in the system.

8) Create a channel called mychannel, carchannel in the deployed network.

9) Take the existing Fabcar smart contract and add a new function to query the car on the basis of person name and deploy the smart contract on the Hyperledger Fabric Network.

10) Write an SDK program to query the person details from the deployed smart.

TEXT BOOK:

1. Blockchain Blue print for Economy by Melanie Swan

REFERENCE:

1. Blockchain Basics: A Non-Technical Introduction in 25 Steps 1st ed. Edition, by Daniel Drescher

CYBER SECURITY (Professional Elective - V)

M.Tech CNIS/CN/CYS II Year I Sem.

L	T	P	C
3	0	0	3

Course objectives:

1. To understand various types of cyber-attacks and cyber-crimes
2. To learn threats and risks within context of the cyber security
3. To have an overview of the cyber laws & concepts of cyber forensics
4. To study the defensive techniques against these attacks

Course Outcomes:

1. Analyze and evaluate the cyber security needs of an organization.
2. Understand Cyber Security Regulations and Roles of International Law
3. Design and develop a security architecture for an organization.
4. Understand fundamental concepts of data privacy attacks

UNIT - 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, Cyber Threats-Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage, etc., Comprehensive Cyber Security Policy.

UNIT - II

Cyberspace and the Law & Cyber Forensics: Introduction, Cyber Security Regulations, Roles of International Law. The INDIAN Cyberspace, National Cyber Security Policy.

Introduction, Historical background of Cyber forensics, Digital Forensics Science, The Need for Computer Forensics, Cyber Forensics and Digital evidence, Forensics Analysis of Email, Digital Forensics Lifecycle, Forensics Investigation, Challenges in Computer Forensics

UNIT - 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, Organizational security Policies and Measures in Mobile Computing Era, Laptops.

UNIT- IV

Cyber Security: Organizational Implications: Introduction, cost of cybercrimes and IPR issues, web threats for organizations, security and privacy implications, social media marketing: security risks and perils for organizations, social computing and the associated challenges for organizations

UNIT - V

Privacy Issues: Basic Data Privacy Concepts: Fundamental Concepts, Data Privacy Attacks, Datalinking and profiling, privacy policies and their specifications, privacy policy languages, privacy in different domains- medical, financial, etc

Cybercrime: Examples and Mini-Cases

Examples: Official Website of Maharashtra Government Hacked, Indian Banks Lose Millions of Rupees, Parliament Attack, Pune City Police Bust Nigerian Racket, e-mail spoofing instances. **Mini-Cases:** The Indian Case of online Gambling, An Indian Case of Intellectual Property Crime, Financial Frauds in Cyber Domain.

TEXT BOOKS:

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.

REFERENCES:

1. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press.
2. Introduction to Cyber Security, Chwan-Hwa(john) Wu,J. David Irwin, CRC Press T&F Group.

NETWORK MANAGEMENT SYSTEMS AND OPERATIONS (Professional Elective - V)

M.Tech CNIS/CN/CYS II Year I Sem.

L	T	P	C
3	0	0	3

Course Objectives:

1. To maintain optimal network performance and availability, and to ensure continuous uptime
2. Monitor the network for problems that require special attention

Course Outcomes:

1. Understand the basic network elements and their services
2. To able to familiarize with different network faults and their correction techniques
3. Understand various measures of network performance

UNIT – I:

The Network Management Challenge: Introduction, The Internet and Network Management, Internet Structure, Managing an Entity, Internal and External policies, The state of Network Management, Network Management in the Gartner Model, Benefits of Automation, The Lack of Industry Response, Impact on Business, Distributed Systems and new abstractions.

A Review of Network Elements and Services: Introduction, Network Devices and Network Services, Network Elements and Element Management, Effect of physical organization on Management, Examples of Network Elements and Services, Basic Ethernet Switch, VLAN Switch, Access Point for a Wireless LAN, Cable Modem System, DSL Modem System and DSLAM, CSU/DSU used in Wide Area Digital Circuits, Channel Bank, IP Router, Firewall, DNS Server, DHCP Server, Web Server, HTTP Load Balancer.

UNIT – II:

The Network Management Problem: Introduction, What is Network Management?, The scope of Network Management, variety and multi-vendor environments, element and network management systems, scale and complexity, types of networks, classification of devices, FCAPS: The Industry Standard Definition, The motivation for automation, Why Automation has not occurred, Organization of management Software.

Configuration and Operation: Introduction, Intuition for configuration, configuration and protocol layering, dependencies among configuration parameters, seeking a more precise definition of configuration, configuration and temporal consequences, configuration and global consistency, global state and practical systems, configuration and default values, partial state, automatic update and recovery, Interface paradigm and incremental configuration, commit and rollback during configuration, automated rollback and timeout, snapshot, configuration, and partial state, separation of setup and activation.

UNIT – III:

Fault detection and correction: Introduction, Network Faults, Trouble Reports, Symptoms, And Causes, Troubleshooting And Diagnostics, Monitoring, Baselines, Items That Can Be Monitored, Alarms, Logs, And Polling, Identifying The Cause Of A Fault, Human Failure And Network Faults, Protocol Layering And Faults, Hidden Faults And Automatic Correction, Anomaly Detection And Event Correlation, Fault Prevention.

Performance Assessment and Optimization: Introduction, aspects of performance, Items that can be measured, measures of network performance, application and endpoint sensitivity, degraded service, variance in traffic and congestion, congestion, delay and utilization, local and end-to-end measurements, passive observation Vs. active probing, bottlenecks and future planning, capacity Planning, planning the capacity of a switch, planning the capacity of a router, planning the capacity of an Internet connection, measuring peak and average traffic on a link, estimated peak utilization and 95th percentile, relationship between average and peak utilization, consequences for management

and the 50/80 Rule, capacity planning for a complex topology, a capacity planning process, route changes and traffic engineering, failure scenarios and availability.

UNIT – IV:

Security: Introduction, The illusion of a secure network, security as a process, security terminology and concepts, management goals related to security, Risk Assessment, Security policies, acceptable use policy, basic technologies used for security, management issues and security, Security architecture: Perimeter Vs. Resources, element coordination and firewall unification, resource limits and denial of service, management of authentication, access control and user authentication, management of wireless networks, security of the network, role-based access control, audit trails and security logging, key management.

Management tools and technologies: Introduction, the principle of most recent change, the evolution of Management tools, management tools as applications, using a separate network for management, types of management tools, physical layer testing tools, reach ability and connectivity tools (ping), packet analysis tools, discovery tools, device interrogation interfaces and tools, event monitoring tools, triggers, Urgency Levels, And Granularity, events, Urgency Levels and traffic, performance monitoring tools, flow analysis tools, routing and traffic engineering tools, Configuration tools, Security Enforcement tools, Network Planning tools, Integration of Management tools, NOCs and Remote Monitoring, Remote CLI Access, Remote Aggregation Of Management Traffic.

UNIT – V:

Network Management Tools: Zabbix Labs, Nagios, Google Cloud network, Automation with Terraform.

TEXT BOOKS:

1. Automated Network Management Systems, D. Comer, Prentice Hall, 2006, ISBN No. 0132393085.
2. Nagios Core Administration Cookbook - Second Edition, Tom Ryder, 2016, Packt publishing, ISBN: 781785889332.
3. Terraform: Up and Running, Yevgeniy Brikman, 2017, O'Reilly Media, Inc., ISBN: 9781491977088.

REFERENCE:

1. Applied Network Security Monitoring, Chris Sanders, Jason Smith, Syngress publications.

VEHICULAR AD-HOC NETWORKS (Professional Elective - V)

M.Tech CNIS/CN/CYS II Year I Sem.

L	T	P	C
3	0	0	3

Course Objectives:

1. To give exposure to state of the art in VANETs
2. To understand VANETs which now open new vistas for internet access, distributed gaming and the fast-growing Mobile entertainment industry.
3. To understand VANETs to promote Traffic Safety.

Course Outcomes:

1. Graduate students and practitioners who intend to do work in VANETs can work on key research challenges.

UNIT - I:

Introduction to Vehicular Ad Hoc Networks (VANETs)

Traffic Monitoring, Causes of congestion, Traffic Monitoring Data, Common Applications of Traffic Data, Commonly used sensor technology, Detection methods

UNIT - II:

Models for Traffic flow and Vehicle Motion

Models for Longitudinal Vehicle Movement, Lane changes situations, Simulating Vehicle-to Vehicle and Infrastructure-to-Vehicle Communication

UNIT - III:

Networking Issues

Routing in MANET, Applicability of MANET Routing to Vehicular Environment, Routing protocols for VANET.

UNIT - IV:

Delay-Tolerant Networks in VANETs

Deterministic/Stochastic Delay-Tolerant Routing, Vehicle Traffic Model, Vehicle- Roadside Data Access, Data Dissemination in VANETs

UNIT - V:

Localization in Vehicular Ad-Hoc Networks

Localization-Aware VANET applications, Localization Techniques for VANETs, Data Fusion in VANET Localization Systems

TEXT BOOKS:

1. Stephan Olariu, Michele C. Weigle, “Vehicular Networks from Theory to Practice”, CRC Press.
2. Hassnaa Moustafa and Yan Zhang, “Vehicular Networks: Techniques, Standards and Applications,” Auerbach Publications, 2009.
3. Selected Papers about Vehicular Ad Hoc Networks (VANETs).

REFERENCES:

1. C. Siva Ram Murthy and B.S. Manoj, “Ad Hoc Wireless Networks: Architectures and Protocols,” Prentice Hall, 2004.
2. William Stallings, “Wireless Communications and Networks,” Prentice Hall, 2004.

IPR (Open Elective)

M.Tech CNIS/CN/CYS II Year I Sem.

L	T	P	C
3	0	0	3

Course Objectives:

1. To explain the art of interpretation and documentation of research work
2. To explain various forms of intellectual property rights
3. To discuss leading International regulations regarding Intellectual Property Rights

Course Outcomes: Upon the Successful Completion of the Course, the Students would be able to:

1. Understand types of Intellectual Property
2. Analyze trademarks and its functionality
3. Illustrate law of copy rights and law of patents

UNIT- I

Introduction to Intellectual property: Introduction, types of intellectual property, international organizations, agencies and treaties, importance of intellectual property rights.

UNIT - II

Trade Marks: Purpose and function of trademarks, acquisition of trade mark rights, protectable matter, selecting, and evaluating trade mark, trade mark registration processes.

UNIT - III

Law of copy rights: Fundamental of copy right law, originality of material, rights of reproduction, rights to perform the work publicly, copy right ownership issues, copy right registration, notice of copy right, international copy right law.

Law of patents: Foundation of patent law, patent searching process, ownership rights and transfer

UNIT - IV

Trade Secrets: Trade secret law, determination of trade secrete status, liability for misappropriations of trade secrets, protection for submission, trade secrete litigation.

Unfair competition: Misappropriation right of publicity, false advertising.

UNIT - V

New development of intellectual property: new developments in trade mark law; copy right law, patent law, intellectual property audits.

International overview on intellectual property, international – trade mark law, copy right law, international patent law, and international development in trade secrets law.

TEXT BOOKS & REFERENCES:

1. Intellectual property right, Deborah. E. Bouchoux, Cengage learning.
2. Intellectual property right – Unleashing the knowledge economy, prabuddha ganguli, Tata McGraw Hill Publishing company ltd.

FAULT TOLERANCE SYSTEMS (Open Elective)

M.Tech CNIS/CN/CYS II Year I Sem.

L	T	P	C
3	0	0	3

Course Objectives:

1. To know the different advantages and limits of fault avoidance and fault tolerance techniques.
2. To impart the knowledge about different types of redundancy and its application for the design of computer system being able to function correctly even under presence of faults and data errors.
3. To understand the relevant factors in evaluating alternative system designs for a specific set of requirements.
4. To understand the subtle failure modes of "fault-tolerant" distributed systems.

Course Outcomes: Upon the Successful Completion of the Course, the Students would be able to:

1. Become familiar with general and state of the art techniques used in design and analysis of fault tolerant digital systems.
2. Be familiar with making system fault tolerant, modeling and testing, and benchmarking to evaluate and compare systems.

UNIT - I

Introduction to Fault Tolerant Computing: Basic concepts and overview of the course; Faults and their manifestations, Fault/error modeling, Reliability, availability and maintainability analysis, System evaluation, performance reliability tradeoffs.

UNIT - II

System level fault diagnosis: Hardware and software redundancy techniques. Fault tolerant system design methods, Mobile computing and Mobile communication environment, Fault injection methods.

UNIT - III

Software fault tolerance: Design and test of defect free integrated circuits, fault modeling, built in self-test, data compression, error correcting codes, simulation software/hardware, fault tolerant system design, CAD tools for design for testability.

UNIT - IV

Information Redundancy and Error Correcting Codes: Software Problem. Software Reliability Models and Robust Coding Techniques, Reliability in Computer Networks Time redundancy. Re execution in SMT, CMP Architectures, Fault Tolerant Distributed Systems, Data replication.

UNIT - V

Case Studies in FTC: ROC, HP Non-Stop Server. Case studies of fault tolerant systems and current research issues.

TEXT BOOK:

1. Fault Tolerant Computer System Design by D. K. Pradhan, Prentice Hall.

REFERENCES:

1. Fault Tolerant Systems by I. Koren, Morgan Kauffman.
2. Software Fault Tolerance Techniques and Implementation by L. L. Pullum, Artech House Computer Security Series.
3. Reliability of Computer Systems and Networks: Fault Tolerance Analysis and Design by M. L. Shooman, Wiley.

INTRUSION DETECTION SYSTEMS (Open Elective)

M.Tech CNIS/CN/CYS II Year I Sem.

L	T	P	C
3	0	0	3

Prerequisites: Computer Networks, Computer Programming

Course Objectives:

1. Compare alternative tools and approaches for Intrusion Detection through quantitative analysis to determine the best tool or approach to reduce risk from intrusion.
2. Identify and describe the parts of all intrusion detection systems and characterize new and emerging IDS technologies according to the basic capabilities all intrusion detection systems share.

Course Outcomes: After completion of the course, students will be able to:

1. Possess a fundamental knowledge of Cyber Security.
2. Understand what vulnerability is and how to address most common vulnerabilities.
3. Know basic and fundamental risk management principles as it relates to Cyber Security and Mobile Computing.
4. Have the knowledge needed to practice safer computing and safeguard your information using
   Digital Forensics.
5. Understand basic technical controls in use today, such as firewalls and Intrusion Detection systems.
6. Understand legal perspectives of Cyber Crimes and Cyber Security.

UNIT - I

The state of threats against computers, and networked systems-Overview of computer security solutions and why they fail-Vulnerability assessment, firewalls, VPN's -Overview of Intrusion Detection and Intrusion Prevention, Network and Host-based IDS

UNIT - II

Classes of attacks - Network layer: scans, denial of service, penetration Application layer: software exploits, code injection-Human layer: identity theft, root access-Classes of attackers-Kids/hackers/sop Hesitated groups-Automated: Drones, Worms, Viruses

UNIT - III

A General IDS model and taxonomy, Signature-based Solutions, Snort, Snort rules, Evaluation of IDS, Cost sensitive IDS

UNIT - IV

Anomaly Detection Systems and Algorithms-Network Behavior Based Anomaly Detectors (rate based)-Host-based Anomaly Detectors-Software Vulnerabilities-State transition, Immunology, Payload Anomaly Detection

UNIT - V

Attack trees and Correlation of alerts- Autopsy of Worms and Botnets-Malware detection - Obfuscation, polymorphism- Document vectors.

Email/IM security issues-Viruses/Spam-From signatures to thumbprints to zero-day detection-Insider Threat issues-Taxonomy-Masquerade and Impersonation Traitors, Decoys and Deception-Future: Collaborative Security

TEXT BOOKS:

1. Peter Szor, The Art of Computer Virus Research and Defense, Symantec Press ISBN 0-321-30545-3.
2. Markus Jakobsson and Zulfikar Ramzan, Crimeware, Understanding New Attacks and Defenses.

REFERENCE BOOKS:

1. Saiful Hasan, Intrusion Detection System, Kindle Edition.
2. Ankit Fadia, Intrusion Alert: An Ethical Hacking Guide to Intrusion Detection.

Online Websites/Materials:

1. https://www.intechopen.com/books/intrusion-detection-systems/

Online Courses:

1. https://www.sans.org/course/intrusion-detection-in-depth
2. https://www.cybrary.it/skill-certification-course/ids-ips-certification-training-course

DIGITAL FORENSICS (Open Elective)

M.Tech CNIS/CN/CYS II Year I Sem.

L	T	P	C
3	0	0	3

Pre-Requisites: Cybercrime and Information Warfare, Computer Networks

Course Objectives:

1. provides an in-depth study of the rapidly changing and fascinating field of computer forensics.
2. Combines both the technical expertise and the knowledge required to investigate, detect and prevent digital crimes.
3. Knowledge on digital forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation, e-discovery tools
4. E-evidence collection and preservation, investigating operating systems and file systems, network forensics, art of steganography and mobile device forensics

Course Outcomes: On completion of the course the student should be able to

1. Understand relevant legislation and codes of ethics.
2. Computer forensics and digital detective and various processes, policies and procedures.
3. E-discovery, guidelines and standards, E-evidence, tools and environment.
4. Email and web forensics and network forensics.

UNIT - I

Digital Forensics Science: Forensics science, computer forensics, and digital forensics.
Computer Crime: Criminalistics as it relates to the investigative process, analysis of cyber criminalistics area, holistic approach to cyber-forensics

UNIT - II

Cyber Crime Scene Analysis:
Discuss the various court orders etc., methods to search and seizure electronic evidence, retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation.

UNIT - III

Evidence Management & Presentation:
Create and manage shared folders using operating system, importance of the forensic mindset, define the workload of law enforcement, Explain what the normal case would look like, Define who should be notified of a crime, parts of gathering evidence, Define and apply probable cause.

UNIT - IV

Computer Forensics: Prepare a case, Begin an investigation, Understand computer forensics workstations and software, Conduct an investigation, Complete a case, Critique a case,
Network Forensics: open-source security tools for network forensic analysis, requirements for preservation of network data.

UNIT - V

Mobile Forensics: mobile forensics techniques, mobile forensics tools.
Legal Aspects of Digital Forensics: IT Act 2000, amendment of IT Act 2008.
Recent trends in mobile forensic technique and methods to search and seizure electronic evidence

TEXT BOOKS:

1. John Sammons, The Basics of Digital Forensics, Elsevier
2. John Vacca, Computer Forensics: Computer Crime Scene Investigation, Laxmi Publications

REFERENCES:

1. William Oettinger, Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence, Packt Publishing; 1st edition (30 April 2020), ISBN: 1838648178.
2. Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar, Cybercrime and Digital Forensics: An Introduction, Routledge.

OPTIMIZATION TECHNIQUES (Open Elective)

M.Tech CNIS/CN/CYS II Year I Sem.

L	T	P	C
3	0	0	3

Prerequisite: Mathematics –I, Mathematics –II

Course Objectives:

1. To introduce various optimization techniques i.e classical, linear programming, transportation problem, simplex algorithm, dynamic programming
2. Constrained and unconstrained optimization techniques for solving and optimizing electrical and electronic engineering circuits design problems in real world situations.
3. To explain the concept of Dynamic programming and its applications to project implementation.

Course Outcomes: After completion of this course, the student will be able to:

1. explain the need of optimization of engineering systems.
2. understand optimization of electrical and electronics engineering problems.
3. apply classical optimization techniques, linear programming, simplex algorithm, transportation problem.
4. apply unconstrained optimization and constrained non-linear programming and dynamic programming.
5. Formulate optimization problems.

UNIT - I

Introduction and Classical Optimization Techniques: Statement of an Optimization problem – design vector – design constraints – constraint surface – objective function – objective function surface - classification of Optimization problems.

Linear Programming: Standard form of a linear programming problem – geometry of linear programming problems – definitions and theorems – solution of a system of linear simultaneous equations – pivotal reduction of a general system of equations – motivation to the simplex method – simplex algorithm.

UNIT - II

Transportation Problem: Finding initial basic feasible solution by north – west corner rule, least cost method and Vogel's approximation method – testing for optimality of balanced transportation problems. Degeneracy.

Assignment problem – Formulation – Optimal solution - Variants of Assignment Problem; Traveling Salesman problem.

UNIT - III

Classical Optimization Techniques: Single variable Optimization – multi variable Optimization without constraints – necessary and sufficient conditions for minimum/maximum – multivariable Optimization with equality constraints: Solution by method of Lagrange multipliers – Multivariable Optimization with inequality constraints: Kuhn – Tucker conditions.

Single Variable Nonlinear Unconstrained Optimization: Elimination methods: Uni Model function-its importance, Fibonacci method & Golden section method.

UNIT - IV

Multi variable nonlinear unconstrained optimization: Direct search methods – Univariant method, Pattern search methods – Powell's, Hooke - Jeeves, Rosenbrock's search methods. Gradient methods: Gradient of function & its importance, Steepest descent method, Conjugate direction methods: Fletcher-Reeves method & variable metric method.

UNIT - V

Dynamic Programming: Dynamic programming multistage decision processes – types – concept of sub optimization and the principle of optimality – computational procedure in dynamic programming – examples illustrating the calculus method of solution - examples illustrating the tabular method of solution.

TEXT BOOKS:

1. Optimization Techniques & Applications by S.S.Rao, New Age International.
2. Optimization for Engineering Design by Kalyanmoy Deb, PHI

REFERENCES:

1. George Bernard Dantzig, Mukund Narain Thapa, “Linear programming”, Springer series in Operations Research 3rd edition, 2003.
2. H. A. Taha, “Operations Research: An Introduction”, 8th Edition, Pearson/Prentice Hall, 2007.
3. Optimization Techniques by Belegundu & Chandrupatla, Pearson Asia.
4. Optimization Techniques Theory and Practice by M.C. Joshi, K.M. Moudgalya, Narosa Publications

CYBER PHYSICAL SYSTEMS (Open Elective)

M.Tech CNIS/CN/CYS II Year I Sem.

L	T	P	C
3	0	0	3

Course Objective: To learn about design of cyber-physical systems

Course Outcomes: Upon the Successful Completion of the Course, the Students would be able to:

1. Understand the core principles behind CPS
2. Identify Security mechanisms of Cyber physical systems
3. Understand Synchronization in Distributed Cyber-Physical Systems

UNIT - I

Symbolic Synthesis for Cyber-Physical Systems

Introduction and Motivation, Basic Techniques - Preliminaries, Problem Definition, Solving the Synthesis Problem, Construction of Symbolic Models, Advanced Techniques: Construction of Symbolic Models, Continuous-Time Controllers, Software Tools

UNIT - II

Security of Cyber-Physical Systems

Introduction and Motivation, Basic Techniques - Cyber Security Requirements, Attack Model, Countermeasures, Advanced Techniques: System Theoretic Approaches

UNIT - III

Synchronization in Distributed Cyber-Physical Systems: Challenges in Cyber-Physical Systems, A Complexity-Reducing Technique for Synchronization, Formal Software Engineering, Distributed Consensus Algorithms, Synchronous Lockstep Executions, Time-Triggered Architecture, Related Technology, Advanced Techniques

UNIT - IV

Real-Time Scheduling for Cyber-Physical Systems

Introduction and Motivation, Basic Techniques - Scheduling with Fixed Timing Parameters, Memory Effects, Multiprocessor/Multicore Scheduling, Accommodating Variability and Uncertainty

UNIT - V

Model Integration in Cyber-Physical Systems

Introduction and Motivation, Causality, Semantic Domains for Time, Interaction Models for Computational Processes, Semantics of CPS DSMLs, Advanced Techniques, ForSpec, The Syntax of CyPhyML, Formalization of Semantics, Formalization of Language Integration.

TEXT BOOKS:

1. Raj Rajkumar, Dionisio De Niz, and Mark Klein, Cyber-Physical Systems, Addison-Wesley Professional.
2. Rajeev Alur, Principles of Cyber-Physical Systems, MIT Press, 2015

GRAPH ANALYTICS (Open Elective)

M.Tech CNIS/CN/CYS II Year I Sem.

L	T	P	C
3	0	0	3

Course Objectives:

1. To explore the concept of Graphs and related algorithms.
2. To learn new ways to model, store, retrieve and analyze graph-structured data.
3. To be aware of advanced concepts in graph analytic techniques and its applications.

Course Outcomes: Upon the Successful Completion of the Course, the Students would be able to:

1. Understand Large-scale Graph and its Characteristics
2. Analyze Breadth-First Search Algorithm
3. Illustrate Recent Advances in Scalable Network Generation

UNIT - I

Introduction and Application of Large-scale Graph: Characteristics, Complex Data Sources - Social Networks, Simulations, Bioinformatics; Categories- Social, Endorsement, Location, Co-occurrence graphs; Graph Data structures, Parallel, Multicore and Graph Algorithms

UNIT - II Algorithms: Search and Paths

A Work-Efficient Parallel Breadth-First Search Algorithm (or How To Cope With the Nondeterminism of Reducers), Multi-Objective Shortest Paths

UNIT - III Algorithms: Structure

Multicore Algorithms for Graph Connectivity Problems, Distributed Memory Parallel Algorithms for Massive Graphs, Massive-Scale Distributed Triangle Computation and Applications

UNIT - IV Models

Recent Advances in Scalable Network Generation, Computational Models for Cascades in Massive Graphs, Executing Dynamic Data-Graph Computations Deterministically Using Chromatic Scheduling.

UNIT - V Frameworks and Software

Graph Data Science Using Neo4j, A Cloud-Based Approach to Big Graphs, Interactive Graph Analytics at Scale in Arkouda

TEXT BOOKS:

1. David A. Bader, Massive Graph Analytics, CRC Press

REFERENCES:

1. Stanley Wasserman, Katherine Faust, "Social Network Analysis: Methods and Applications", (Structural Analysis in the Social Sciences), Cambridge University Press, 1995.
2. Matthew O. Jackson, “Social and Economic Networks”, Princeton University Press, 2010.
3. Tanja Falkowski, "Community Analysis in Dynamic Social Networks", (Dissertation), University Magdeburg, 2009.