DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, MIT Manipal

M.Tech. COMPUTER SCIENCE AND INFORMATION SECURITY

Program Structure (Applicable to 2023 admission onwards)

YEAR	FIRST SEMESTER						SECOND SEMESTER					
	SUB CODE	**SUBJECT NAME**	**L**	**T**	**P**	**C**	**SUB CODE**	**SUBJECT NAME**	**L**	**T**	**P**	**C**
I	MAT ****	COMPUTATIONAL METHODS & STOCHASTIC PROCESSES	4	0	0	4	CSE ****	BLOCKCHAIN TECHNOLOGY AND APPLICATIONS	3	1	0	4
	HUM ****	RESEARCH METHODOLOGY AND TECHNICAL COMMUNICATION	1	0	3	-	CSE ****	ETHICAL HACKING	3	1	0	4
	CSE ****	SYSTEMS AND NETWORK SECURITY	4	0	0	4	CSE ****	ELECTIVE I	4	0	0	4
	CSE ****	ADVANCED DATA STRUCTURES AND ALGORITHMS	3	1	0	4	CSE ****	ELECTIVE II	4	0	0	4
	CSE ****	DESIGN OF SECURE PROTOCOLS	3	1	0	4	CSE ****	ELECTIVE III	4	0	0	4
	CSE ****	ADVANCED CRYPTOGRAPHY AND CRYPTANALYSIS	3	1	0	4	*** ****	OPEN ELECTIVE	3	0	0	3
	CSE ****	SYSTEMS AND NETWORK SECURITY LAB	0	0	3	1	HUM ****	RESEARCH METHODOLOGY AND TECHNICAL COMMUNICATION	1	0	3	2
	CSE ****	ADVANCED DATA STRUCTURES AND ALGORITHMS LAB	0	0	3	1	CSE ****	ETHICAL HACKING LAB	0	0	3	1
	CSE ****	ADVANCED CRYPTOGRAPHY AND CRYPTANALYSIS LAB	0	0	3	1	CSE ****	BLOCKCHAIN TECHNOLOGY LAB	0	0	3	1
	Total		**18**	**3**	**12**	**23**			**22**	**2**	**9**	**27**
II	CSE 6098	PROJECT WORK							**0**	**0**	**0**	**25**

PROGRAM ELECTIVES		OPEN ELECTIVES	
	PROGRAM ELECTIVE I	CSE ****	APPLIED DATA SCIENCE
CSE ****	WIRELESS SECURITY	CSE ****	APPLIED NATURAL LANGUAGE PROCESSING
CSE ****	INFORMATION SECURITY MANAGEMENT	CSE ****	INTRODUCTION TO DEEP LEARNING (Offered to Non CSE/CSIS students)
CSE ****	CYBER FORENSICS		
	PROGRAM ELECTIVE II		
CSE ****	AI AND ML TECHNIQUES IN CYBERSECURITY		
CSE ****	MULTIMEDIA SECURITY		
CSE ****	DATABASE AND APPLICATION SECURITY		
	PROGRAM ELECTIVE III		
CSE ****	WEB TECHNOLOGIES AND APPLICATIONS		
CSE ****	QUANTUM COMPUTING		
CSE ****	SOFTWARE PROJECT MANAGEMENT		
CSE ****	DEEP LEARNING AND APPLICATIONS		

SEMESTER I

MAT **** COMPUTATIONAL METHODS AND STOCHASTIC PROCESSES [4 0 0 4]

Optimization Techniques in Game Theory: Maximin-Minimax Principle, Graphical method, Dominance method, Optimization Techniques in Linear Programming: Mathematical modelling, Graphical method, Simplex method, Two-Phase method, Probability: Distributions, Covariance, Correlation, Sampling, Estimation in statistics, Testing of hypothesis, Bayesian Hypothesis, Stochastic Processes: Stationary process, Autocorrelation problems, Power density technique, Markov model, Classification of chains, Higher transition probabilities, Limiting behaviour, Linear Algebra: Orthonormal matrices, Gram Schmidt orthonormalization process, QR decomposition, SVD, Graph Theory: Walk, Connectedness, Minimum spanning trees, Connected components, Shortest Path method techniques, Advanced Numerical Methods: Boundary value problem, Finite difference method and Finite element method.

References:

1. G. Hadely, Linear Algebra, Addison-Wesley publishing company, Singapore (1961).
2. A. Papoulis & S. U. Pillai, Probability, Random Variables and Stochastic Processes, McGraw Hill (2002).
3. P. Z. Peebles Jr., Probability, Random Variables and Random Signal Principles, McGraw Hill International Edition, Singapore. (2001).
4. B. Carnahan, H. A. Luther, and J. O. Wilkes, Applied Numerical Methods, John Wiley & sons (1969).
5. H. A. Taha, Operational Research-An Introduction, Pearson Education, Edn 10 (2019).
6. F. Haray, Graph Theory, Narosa Publishing House (2001).
7. J. Medhi, Stochastic Processes, New Age International Publishers, Edn 3 (2009).

Course Outcomes:

After completing the course, the student will be able to:

1. Analyse optimization problems using game theory and simplex method.
2. Apply probability concepts in data analysis problems.
3. Analyse stochastic processes and Markov Chain Models.
4. Apply different decomposition techniques to eliminate the less important data in the matrix to produce a low-dimensional approximation.
5. Apply different techniques from graph theory in engineering problems.
6. Apply advanced numerical methods to engineering problems related to partial differential equations.

HUM **** RESEARCH METHODOLOGY AND TECHNICAL PRESENTATION [1 0 3 2]

Theory: Introduction, Types of research and Significance of research, The research process: The eight-step model. Reviewing the literature and summarizing the literature. Formulating a research problem: Identifying variables and hypotheses development. Research Design, Measurement scales, Data collection-primary and secondary sources of data, Establishing reliability and validity of research instrument. Sampling- types of sampling techniques, Ethical issues in data collection, processing data and displaying data. Writing a research proposal, Writing a research report, Presentation of figures and tables. Referencing-IEEE, APA and Harvard style of referencing. Making an effective technical presentation.

Lab exercises: The students are expected to conduct following tasks. Conduction of Literature review, Formulation of Research Problem through literature review, Developing conceptual framework and Hypothesis Development, Designing Research Methodology, Development of Research Instrument- Questionnaire, Development of Research Proposal, Presentations and evaluation.

References

1. Dr. Ranjit Kumar, Research Methodology: A step by step guide for beginners, SAGE, 4th edition. 2015.
2. Geoffery R. Marczyk, David DaMatteo & David Festinger, Essentials of Research Design and Methodology, John Wiley & Sons, 2004.
3. John W. Creswel, Research Design: Qualitative, Quantitative and Mixed Method Approaches, SAGE 2004.
4. Donald R Cooper & Pamela S Schindler, Business Research Methods, McGraw Hill International, 2007.
5. C. R. Kothari, Research Methodology: Methods and Techniques, New Age International Publisher, 2008.

Course Outcomes:

After completing the course, the student will be able to:

1. Define concept of research and recall types of research.
2. Define the problem and develop the research design to solve the problem
3. Organize a thesis report and a manuscript
4. Develop effective technical presentation
5. Develop a good research proposal

CSE XXXX: SYSTEMS AND NETWORK SECURITY [4 0 0 4]

Introduction: CIA Triad, Defence Models, Computer Viruses: Genesis, Classification. Risk analysis: Threats, types of attacks, worms, trojans, buffer overflow, poisoning, risk analysis. Intrusion detection systems, types, changing nature of IDS tools, challenges, implementation, intrusion prevention systems, intrusion detection tools. Operating system security: OS models, classic security models, reference monitor, international standards for operating system security. Firewalls: Types, implementation, Demilitarized Zone, Firewall forensics, Firewall Services and Limitations. IPSec: IPv4 and Ipv6, SKIP, IKE phases, Session Keys, Message IDs, Phase 2/Quick Mode, Traffic selectors, IPSec SA. PGP: Overview, Key distribution, Efficient encoding, Signature Types, Key rings, Anomalies and Object formats. Kerberos: Version 4, Realms, Interrealm authentication, Message formats. Kerberos V5 ASN.1, KDC Database, Kerberos V5 Messages.

References:

1. Mark Rhodes Ousley, “The Complete Reference: Information Security”, (2e), Mc Graw HillPublication, 2013.
2. Peter Szor, “The art of Computer Virus Research and Defense”, Addison Wesley Professional, 2005.
3. Joseph Migga Kizza, “Guide to Computer Security”, (3e), Springer,2015.
4. Charlie Kaufman, Radia Perlman, Mike Speciner, “Network Security : PRIVATE Communication in a PUBLIC World”, (2e), Pearson Education, 2005.
5. William Stallings, “Cryptography and Network Security Principles and Practice”, (6e), Prentice Hall, 2014.

Course Outcomes:

After completing the course, the student will be able to:

1. Summarize defence models, security risks and different types of viruses.
2. Identify system intrusion and apply prevention methods.
3. Analyse OS security models and construct firewall policies.
4. Identify different modes of security at the ip layer.
5. Apply protocols for authentication and e-mail security.

CSE XXXX: ADVANCED DATA STRUCTURES AND ALGORITHMS [3 1 0 4]

Amortized Analysis: Aggregate analysis, The Aggregate analysis, The accounting method, The potential method, Dynamic Tables. B-Trees: Basic operations on B-Trees, Deleting a key from a

B-Tree. Binomial trees and Binomial heaps: Operations on Binomial heaps. Structure of Fibonacci heaps, Mergeable heap operations, Decreasing a key and deleting a node. The van Emde Boas Tree: Preliminary approaches, A recursive structure, Disjoint-set operations: Linked-list representation of disjoint sets, Disjoint set forests. Single-Source Shortest Path: The Bellman-Ford algorithm, Single-source shortest paths in directed acyclic graphs, Difference constraints and shortest paths. All-Pairs Shortest Paths: shortest Paths and matrix multiplication, Johnson's algorithm for sparse graphs. Maximum Flow: Flow Networks, The Ford-Fulkerson method, Maximum Bipartite Matching, Multithreaded Algorithms: The basics of dynamic multithreading, Multithreaded matrix multiplication, Multithreaded merge sort. SDL:Probabilistic analysis and randomized algorithms, linear programming. Approximation algorithms

References:

1. Cormen Thomas H., Leiserson Charles E, Rivest Ronald L. and Stein Clifford, "Introduction to Algorithms", (3e), MIT Press, 2009.
2. Cormen Thomas H., Leiserson Charles E, Rivest Ronald L. and Stein Clifford, "Introduction to Algorithms" (2e), Prentice-Hall India, 2001.
3. Baase Sara and Gelder A.V., "Computer Algorithms -Introduction to Design and Analysis", (3e), Pearson Education, 2000
4. Anany Levitin, "Introduction to the Design and Analysis of Algorithms," (3e), Pearson Education, 2011
5. Eli Upfal , Michael Mitzenmacher, " Probability and Computing: Randomization and Probabilistic Techniques in Algorithms and Data Analysis,2017
6. Ding-Zhu Du, Ker-I Ko, Xiaodong Hu, " Design and Analysis of Approximation Algorithms", Springer,2011

CSE XXXX: DESIGN OF SECURE PROTOCOLS [3 1 0 4]

Introduction of Cryptographic Protocols, Background of Cryptographic Protocols, Preliminaries, Cryptographic primitives, Cryptographic protocols, Security of cryptographic protocols, Communication threat model, Introduction of engineering principles, Protocol engineering requirement analysis, Detailed protocol design, Informal Analysis Schemes of Cryptographic Protocols, The security of cryptographic protocols, Security mechanism based on trusted freshenss, Analysis of classic attacks, Security Analysis of Real World Protocols, Secure Socket Layer and Transport Layer Security, Kerberos—the network authentication protocol, Guarantee of Cryptographic Protocol Security, Security definition of authentication, Authentication based on trusted freshness, Formalism of Protocol Security Analysis, BAN logic, Model checking, Belief multisets based on trusted freshness, Automated Analysis of Cryptographic Protocols, Based on Trusted Freshness, Introduction to programming frameworks for design of secured protocols, Comparison of two initial implementations of BMF. SDL: Encryption and Decryption, Vulnerable network, OSI Model, Packet structures, Client-Server computing [5]

References

1. Ling Dong and Kafei Chen, Cryptographic Protocol: Security Analysis based on trusted Freshness, Springer, 2012
2. Goyal, D., Balamurugan, S., Peng, S. L., & Verma, O. P. (Eds.). (2020). Design and Analysis of Security Protocol for Communication. John Wiley & Sons.
3. Maleh, Y. (Ed.). (2018). Security and privacy management, techniques, and protocols. IGI Global.
4. Forouzan, B. A., & Mukhopadhyay, D. (2015). Cryptography and network security (Vol. 12). New York, NY, USA:: Mc Graw Hill Education (India) Private Limited
5. Pachghare, V. K. (2019). Cryptography and information security. PHI Learning Pvt. Ltd.

Course Outcomes:

After completing the course, the student will be able to:

1. Summarize the background of cryptographic protocols
2. Understand engineering principles in designing a security protocol from software engineering perspective
3. Understand the formal and informal methods of analyzing the security of protocol
4. Analyze the real-world protocols and their design
5. Design and present a simple secure protocol using the existing frameworks

CSE ****: ADVANCED CRYPTOGRAPHY AND CRYPTANALYSIS [3 1 0 4]

Overview of symmetric and asymmetric encryption schemes, Cryptanalysis of classical ciphers, attacks on modern block ciphers, Linear and Differential cryptanalysis, Pseudorandom and true random number generators, stream ciphers, Correlation attacks, Attacks on public key cryptosystems- Sieve Algorithms, Primality test algorithms, Factorization Algorithms, Random Oracle and hash functions, MACs, Birthday Attacks, Digital signatures, Attacks on digital signatures, Identity based public key cryptography, Oblivious Transfer and Signatures, Esoteric Protocol, Key Management and Distribution, User Authentication, Federated and Personal Identity Management, Secure Multipart authentication, Probabilistic encryption, Quantum computing cryptography, Application of cryptography and cryptanalysis in real life problems.
SDL: Lightweight cryptosystems, cryptanalysis of light weight ciphers, Slide attacks on block ciphers, Authenticated encryption

References:

1. William Stallings, Cryptography and Network Security – Principles and Practice, (7e), Pearson, 2017
2. Arno Mittelbach, Marc Fischlin, The Theory of Hash Functions and Random Oracles -An Approach to Modern Cryptography' Springer, 2021
3. Joachim von zur Gathan, CryptoSchool, Springer , 2015
4. Antoine Joux, Algorithmic Cryptanalysis, CRC Press, 2009
5. Gildas Avoine, Orhun Kara (Eds), Lightweight Cryptography for Security and Privacy, Conference Proceedings, 2nd International Workshop, LightSec 2013, Springer

Course Outcomes:

After completing the course, the student will be able to:

1. Summarize the different symmetric and asymmetric ciphers and their cryptanalysis
2. Compare the hashing, message authentication codes and digital signature schemes
3. Analyse different authentication mechanisms
4. Apply the birthday paradox for cryptanalysis on hash functions
5. Demonstrate the concepts of key management and distribution
6. Outline the application of cryptography and cryptanalysis in real life problems

CSE ****: CRYPTANALYSIS LAB [0 0 3 1]

Cryptanalysis of classical ciphers and modern symmetric ciphers, hashing, RSA using CrypTool Simulator, Implementation of factorization, sieve, discrete logarithms, Birthday based algorithms, Miniproject

References:

1. Joachim von zur Gathan, CryptoSchool, Springer , 2015
2. Boris S. Verkhovsky, Integer Algorithms in Cryptology and Information Assurance, World Scientific Publishing Company, 2014

Course Outcomes:

After completing the course, the student will be able to:

1. Use CrypTool to analyse the attacks on different ciphers
2. Implement algorithms to cryptanalyse symmetric and asymmetric cryptosystems
3. Implement miniproject

CSE **** ADVANCED DATA STRUCTURES AND ALGORITHMS LAB [0 0 3 1]

Experiments based on theory covered in Advanced data structures. In the latter half of this lab, students will be working on more complex problems.

CSE **** SYSTEMS AND NETWORK SECURITY LAB [0 0 3 1]

Experiments based on theory covered in systems and network security. Experiments on Network monitoring, capturing network traffic and analysis of network protocols using various tools such as wireshark, tcpdump etc. Experiments on secure configuration of network routers, network access points and switches, configuration of e-mail servers, DNS, FTP and web servers, Experiments on host and network security. Experiments on OS security configuration in various operating systems.

SEMESTER II

CSE XXXX: BLOCKCHAIN TECHNOLOGY AND APPLICATIONS [3 1 0 4]

Introduction to Blockchain, Business Use Cases, Technology Use Cases, Legal and Governance Use Cases, Technology on Ethereum, Fast-Track Application Tutorial, Ethereum Application Best Practices, Private Blockchain Platforms and Use Cases, Challenges, Sample Application: Blockchain and Betting, Deploying the Sample Application: Blockchain and Betting, Opportunities and Challenges. Fundamental concepts and applications of Blockchain enabled fog and edge computing: Blockchain Internet of Things (B-IoT), Smart City, e-challan, Developing Governance structure for Blockchain networks, Building a team to drive Blockchain Projects, Understanding Financial Models, Investment rubrics, and model risk frameworks, Blockchain in Logistics and examples across industries.
SDL: Looking ahead: What is a future world.

References:

1. Joseph J. Bambara Paul R. Allen, Blockchain A Practical Guide to Developing Business, Law, and Technology Solutions, McGraw-Hill Education, 2018
2. Dr. Muhammad Maaz Rehan and Dr. Mubashir Husain Rehmani. Blockchain-enabled Fog and Edge Computing Concepts, Architectures, and Applications, (1e) CRC Press, 2021
3. Jai Singh Arun, Jerry Cuomo, Nitin Gaur. Blockchain for Business, Pearson Education, Inc., 2019
4. Matthias Heutger, & Dr. Markus Kückelhaus. BLOCKCHAIN IN LOGISTICS, Accenture Digital, 2018

Course Outcomes:

1. To comprehend the basic concepts of blockchain technology and use cases.
2. To comprehend the Technology on Ethereum and Fast-Track Application implementation.
3. Ability to apply the concepts on fog and edge computing such as B-IoT, Smart city and e-challan
4. To analyse and deployment of Ethereum blockchain technology.
5. To extract information from Blockchain in Logistics and examples across industries

CSE XXXX: ETHICAL HACKING [3 1 0 4]

Introduction to ethical hacking. Fundamentals of computer networking. Introduction to network security. Information gathering, Vulnerability assessment, System hacking: password cracking, penetration testing, etc., Social engineering attacks. Malware threats, Introduction to cryptography, Steganography, biometric authentication, lightweight cryptographic algorithms, Sniffing: Wireshark, ARP poisoning, DNS poisoning. Hacking wireless networks, Denial of service attacks, Elements of hardware security, hacking web applications: vulnerability assessment, SQL injection, cross-site scripting, 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. Cyberspace and the Law & Cyber Forensics: Cyber Security Regulations, Roles of International Law. The INDIAN Cyberspace, National Cyber Security Policy.The Need for Computer Forensics, Cyber Forensics and Digital evidence.

Cybercrime: 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.

Cyber Security: Organizational Implications: Introduction, cost of Cybercrime 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.

References:

1. Erickson, J. (2008). Hacking: the art of exploitation. No starch press.
2. Graves, K. (2010). CEH certified ethical hacker study guide. John Wiley & Sons.
3. Nina Godbole and SunitBelpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley
4. B.B.Gupta,D.P.Agrawal,HaoxiangWang,ComputerandCyberSecurity:Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335, 2018
5. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRCPress
6. Introduction to Cyber Security, Chwan-Hwa(john) Wu,J. David Irwin, CRC Press T&FGroup.

Course Outcomes:

After completing the course, the student will be able to:

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

CSE XXXX: BLOCKCHAIN TECHNOLOGY AND APPLICATIONS LAB [0 0 3 1]

Experiments based on theory covered in Block chain technology. In the latter half of this lab, students will be working on more complex problems.

References:

1. Joseph J. Bambara Paul R. Allen, Blockchain A Practical Guide to Developing Business, Law, and Technology Solutions, McGraw-Hill Education, 2018
2. Dr. Muhammad Maaz Rehan and Dr. Mubashir Husain Rehmani. Blockchain-enabled Fog and Edge Computing Concepts, Architectures, and Applications, (1e) CRC Press, 2021
3. Jai Singh Arun, Jerry Cuomo, Nitin Gaur. Blockchain for Business, Pearson Education, Inc., 2019
4. Matthias Heutger, & Dr. Markus Kückelhaus. BLOCKCHAIN IN LOGISTICS, Accenture Digital, 2018

Course Outcomes:

1. To implement basic concepts of blockchain technology and use cases.
2. To comprehend the Technology on Ethereum and Fast-Track Application implementation.
3. To analyse and deployment of Ethereum blockchain technology.

CSE XXXX: ETHICAL HACKING LAB

Penetration Testing Tools, Packet Snipping Tools, Firewall Configurations, Different types of Foot-printing, Google hacking, Variety of Scanners, Exploits, Dos, Proxy, Password Guessing-How to guess a strong password, Phishing, Sniffer, Session Hijacking, Virus: Virus creating tools, Ransomware, Key logger, Trojan, Rat, Proactive defense, and countermeasures, Incidence Response and Management.

References:

1. Erickson, J. (2008). Hacking: the art of exploitation. No starch press.
2. Graves, K. (2010). CEH certified ethical hacker study guide. John Wiley & Sons.
3. Nina Godbole and SunitBelpure, Cyber Security Understanding Cyber Crimes,Computer Forensics and Legal Perspectives,Wiley
4. B.B.Gupta,D.P.Agrawal,HaoxiangWang,ComputerandCyberSecurity:Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335,2018
5. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRCPress
6. Introduction to Cyber Security, Chwan-Hwa(john) Wu,J. David Irwin, CRC Press T&FGroup.

Course Outcomes:
After completing the course, the student will be able to:

1. Know about the network security issues in different types of network devices.
2. Know how to setup a firewall on Operating System
3. Understand the security and privacy features and operation of browsers.
4. Identify different types of Web Application Vulnerability
5. Point out the vulnerabilities in TCP/IP Protocols used for communications.

CSE XXXX: WIRELESS SECURITY [4 0 0 4]

Introduction and Overview of Wireless Networks, WLAN Security : WEP, TKIP, AESCCMP, RADIUS, TLS, TLS over EAP, Kerberos, LEAP, PEAP, EAP-SIM, Network & Security Architecture, Network Planning & Analysis, Security considerations for various layers of the wireless protocol stack, Cross-layer attack and defense. Enterprise Wireless LAN security, Trust and reputation management, Synchronization & Localization based attacks and mitigation strategies, Smart Grid security, Telecom system and infrastructure attacks, Mobile App and OS security, PAN security, Security in WSN: Overview, Types and Challenges. Design of Wireless Sensor Network for emerging scenarios. SDL: Design analysis of transition from WSN to IoT. IoT security

References:

1. Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, and Mika Ylianttilaa comprehensive Guide to 5G security, Wiley, First Edition, 2018.
2. William A. Arbaugh and Jon Edney, “Real 802.11 Security: Wi-Fi Protected Access and 802.11I”, First Edition,Pearson Education, 2011.
3. W. Stallings, Cryptography and Network Security: Principles and Practice, Pearson, 2014
4. Frank Adelstein, Sandeep KS Gupta, Golden Richard, Fundamentals of Mobile and Pervasive Computing, McGraw-Hill, 2005
5. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security: PRIVATE Communication in a PUBLIC world”, Second Edition, Prentice Hall, 2002
6. Ali Dehghantanha & Kim-Kwang Raymond Choo, Handbook of Big Data and IoT Security, ISBN 978-3-030-10543-3 , 2019

After completing the course, the student will be able to:

1. Understanding and appreciation of the nature and kind of threats, vulnerabilities and defences in various wireless networks and technologies

2. Appreciation for the basics of network security as applied to WLAN
3. To understand the security issues and solutions in wireless sensor networks.
4. Familiarity with the cross-layer attack and defence strategies in wireless networks and systems
5. Ability to understand the Security requirements in IoT.

CSE **** INFORMATION SECURITY MANAGEMENT [4 0 0 4]

What is security? CNSS Security Model, Components of an Information System, Approaches to Information Security Implementation, Intrusion Detection, Password management, Malicious Software-Types, Viruses, Viruses Countermeasures, Introduction, Intruders, Intrusion Detection, Password management, Malicious Software-Types, Viruses, Viruses Countermeasures, Worms, Risks, Security, and Disaster Recovery: Worldwide Host: Battling Back from Attacks, Risks to Information Systems, Security Measures, Firewalls and Proxy Servers, Authentication and Encryption, The Downside of Security Measures, Recovery Measures, Information Security and Risk Management, Security Management Concepts and Principles, Access Control, Security Architecture and Design, Principles of Computer and Network Organizations, Architectures, and Designs, Legal Regulations, Compliance and Investigation, SDL: Intrusion detection system, information system management, network security management

References:

1. William Stallings- “Cryptography and Network Security: Principles and Practice”, Prentice Hall, 5th edition, 2010.
2. Michael E. Whitman and Herbert J. Mattord- “Principles of Information Security”, Cengage Learning India Publication, 4th edition, 2011.
3. EFFY OZ. “Management Information Systems”, 6th edition, 2009
4. Harold F. Tipton, CISSP . Micki Krause, CISSP. “Information Security Management Handbook”, 6th Edition, 2008

Course Outcomes:

After completing the course, the student will be able to:

1. Identify issues of privacy, authenticity, and security of information
2. Recognize the major information security threats and countermeasures
3. Analyze various solutions available for secure multilevel database design
4. Identify network security threats and determine efforts to counter them
5. Understand and analyse the risk in information security systems

CSE XXXX: CYBER FORENSICS [4 0 0 4]

Introduction to Cybercrime, Types of Cybercrime, Extent of Cybercrime, Classification of Cybercrime, Cybercrime—The Present and the Future. Introduction to Cyber Forensics, Cyber Forensics—The Present and the Future, Digital Evidence, Acquisition and Handling of Digital Evidence, Analysis of Digital Evidence, Admissibility of Digital Evidence, Summary of Investigation Process Involving Digital Evidence, Cyber Laws.
SDL: National and International Case Studies: Cybercrime against Individual, Property and Nation.

References:

1. Dejey and Murugan, “Cyber Forensics”, Oxford University Press, 1st Edition, 2018
2. Clint P. Garrison, Digital Forensics for Network, Internet, and Cloud Computing, Elsevier Inc., 2010
3. Investigating Network Intrusions and Cybercrime, EC-Council Press, Cengage Learning, 2010
4. Janine Kremling, & Amanda M. Sharp Parker, Cyberspace, Cybersecurity, and Cybercrime, SAGE Publications, Inc., 2018
5. Dr. Darren R. Hayes, “A Practical Guide to Computer Forensics Investigations”, Pearson Education, Inc., 2015.
6. Eoghan Casey, “Digital evidence and Computer Crime”, Academic Press, 3rd Edition, 2011.
7. Marjie Britz, “Computer Forensics and Cyber Crime”, Pearson, 3rd Edition, 2013.

Course Outcomes:

1. To Utilize a systematic approach to computer investigations.
2. To Identify and develop the applications in the field of Cyber Forensics.
3. To Utilize various Cyber Forensics tools to collect digital evidence.
4. To Perform digital forensics analysis upon networks and network devices.
5. To Perform web-based investigations.

CSE XXXX: AI AND ML TECHNIQUES IN CYBERSECURITY [4 0 0 4]

Why Machine Learning and Security?, Classifying and Clustering, Anomaly Detection, Malware Analysis, Network Traffic Analysis, Protecting the Consumer Web, Production Systems, Adversarial Machine Learning. OWL Ontologies in Cybersecurity: Conceptual Modelling of Cyber-Knowledge, Knowledge Representation of Network Semantics for Reasoning-Powered Cyber-Situational Awareness, The Security of Machine Learning Systems, Patch Before Exploited: An Approach to Identify Targeted Software Vulnerabilities, Applying Artificial Intelligence Methods to Network Attack Detection, Machine Learning Algorithms for Network Intrusion Detection.

References:

1. Clarence Chio and David Freeman, Machine Learning and Security: Protecting Systems with Data and Algorithms, (1e), O'Reilly Media, Inc., 2018.
2. Leslie F. Sikos , AI in Cyber Security, Intelligent Systems Reference Library, Volume 151, Springer Nature Switzerland AG 2019.
3. Abhishek Verma, Jitendra Kumar, Hari Mohan Gaur, Vrijendra Singh, and Valentina Emilia Balas, Advances in Cyber Security and Intelligent Analytics, (1e), CRC Press, Taylor & Francis Group 2023.
4. Roman V. Yampolskiy, Artificial Intelligence Safety and Security, CRC Press, Taylor & Francis Group, 2019.
5. YVONNE R. MASAKOWSKI, Artificial Intelligence and Global Security: Future Trends, Threats and Considerations, (1e), Emerald Publishing Limited, 2020.
6. Padmavathi Ganapathi & D. Shanmugapriya, Handbook of Research on Machine and Deep Learning Applications for Cyber Security, IGI Global, 2020.
7. Brij B. Gupta & Michael Sheng, Machine Learning for Computer and Cyber Security Principles, Algorithms, and Practices, CRC Press, Taylor & Francis Group, 2019.

Course Outcomes:

After completing the course, the student will be able to:

1. Analyze and assess the quality, effectiveness, and robustness of a machine learning model.
2. Demonstrate a broad understanding of common cyber security tasks (e.g., detecting threats, predicting attacks).
3. Design, analyze, and evaluate an appropriate machine learning method for a given cyber security problem.
4. Recognize knowledge representation in network semantics and artificial intelligence methods for network intrusion detection.
5. Identify conceptual cyber-knowledge in cybersecurity and machine learning methods for network intrusion detection.

CSE ****: MULTIMEDIA SECURITY [4 0 0 4]

Fundamentals, Fingerprinting basics, Marking assumption, Collusion attack, Frame proof and anti-collusion codes; Semi-fragile fingerprinting, Multicast fingerprinting problem, Efficient security architectures, Chameleon cipher; Joint fingerprinting and decryption framework; Multimedia encryption, Multimedia compression technologies and standards; Image and Video encryption schemes, Chaotic maps, Transform domain encryption, Huffman tree mutation; Streaming media encryption: Scalable video protection; Multimedia authentication: Watermarking based authentication, attacks and tools, watermarking based on genetic algorithms, Reversible watermarking, high capacity watermarking, visual cryptography, classification, algorithms, Improving visual quality for share images, Copyright protection, , video authentication, Key management for multimedia access and distribution, Zero knowledge protocols, Anonymous fingerprinting, Securing data in healthcare systems and other real life applications

References:

8. Kaiser J. Giri, Shabir Ahmad Parah, Rumaan Bashir, Khan Muhammad, Multimedia Security Algorithm Development, Analysis and Applications, Springer, 2021
9. Bhaskar Mondal, Shyam Singh Rajput, Multimedia Security, Tools, Techniques, and Applications, Apple Academic Press 2023
10. Bin Yan, Yong Xiang, Guang Hua, Improving Image Quality in Visual Cryptography' Springer, 2020
11. WeiQi Yan, Johnathon Weir, Fundamentals of Media Security, Ventus Publishing Aps, 2010
12. Frank Y. Shih, Digital Watermarking and Steganography Fundamentals and Techniques,(2e), CRC Press, 2020

Course Outcomes:

After completing the course, the student will be able to:

1. Analyse the fingerprinting mechanisms and the attacks that could be performed
2. Compare the various multimedia compression technologies and standards
3. Apply chaotic maps and transformations to streaming media encryption
4. Demonstrate the watermarking- based authentication schemes
5. Describe the key management and distribution schemes for multimedia access for cryptanalysis
6. Outline the application of multimedia security in real life problems

CSE 5XXX DATABASE AND APPLICATION SECURITY [4 0 0 4]

Introduction, Database security, Operating systems overview, security environment, Authentication methods, Vulnerabilities of operating systems, Defining and using profiles, Designing and implementing password policies, Granting and revoking user privileges, Obfuscate application code, Secure the database from SQL injection attacks, Beware of double whammies: Combination of SQL injection and buffer overflow vulnerability, Types of users, security models, application types, application security models and Data encryption, Implementing VPD, Implementing oracle VPD, Auditing overview, environment, process, objectives, classification and types, Benefits and side effects of auditing, Map data sources and sinks, Understand Web services security before exposing Web services endpoints, Auditing Database Activities: Introduction, usage of database activities, creating DLL triggers, auditing database activities with oracle, Security and Auditing project cases: Introduction, Case Study for developing an online database.

References:

1. Hassan A. Afyouni, Database Security and Auditing, India Edition, CENGAGE Learning, 2009.
2. RonBen Natan, Implementing Database Security and Auditing, Elsevier, Indian Reprint, 2006.
3. M.TamerÖzsu, Patrick Valdureiz, Principles of Distributed Database Systems, Prentice Hall, (2e), Springer, 2011.
4. Castano, Fugini, Database Security, Addison Wesley, ACM, 2004.
5. Clark, Holloway, The Security Audit and Control of Databases, List, UK, Ashgate, 2011.
6. Douglas, Security and Audit of Database System, Blackwell, UK, 2010.
7. Fernandez, Summers, Wood, Database Security and Integrity, Addison Wesley, 2012.

Course Outcomes:

1. After completing the course, the student will be able to:
2. Explain Security Architecture and Applications.
3. Analyze Authentication and its applications.
4. Explain properties of databases in terms of authentication.
5. Analyze Models for Security Applications.
6. Explain Framework for Security

CSE XXXX: WEB TECHNOLOGIES AND APPLICATIONS [4 0 0 4]

Web development with HTML, CSS, JavaScript, HTML5, Front end web UI frameworks, bootstrap, Bootstrap javascript components, Front end web development with react, react components with JSX, React router, react forms, flow architecture, Redux, Introduction to Redux overview of the Flux architecture, Server side development with NodeJS, Express and MongoDB, REST API using express, interact with MongoDB from a Node application, data storage with MongoDB, Mongoose ODM.

References

1. Frank Zammetti, Modern Full-Stack Development: Using TypeScript, React, Node.js, Webpack, and Docker, APress publication, 2020.
2. Chris, The Full Stack Developer, APress publication, 2018.
3. Juha Hinkula, Hands-On Full Stack Development with Spring Boot 2 and React: Build modern and scalable full stack applications using Spring Framework 5 and React with Hooks, 2nd Edition, Packt publishing, 2019.
4. Nadar Dabit, Full Stack Serverless: Modern Application Development with React, AWS, and GraphQL Greyscale Indian Edition, 2020.

Course Outcomes:

At the end of the course students will be able to

1. Apply the knowledge of web development using HTML, CSS and Javascript to the real-world problem.
2. Apply the knowledge of front-end web UI framework for developing good UI framework for industry related problems.
3. Apply the knowledge of React for web related problems.
4. Apply the knowledge of development with NodeJS and Express for real world problems.
5. Apply the knowledge of MongoDB to design efficient and scalable data models in MongoDB.

CSE XXXX: QUANTUM COMPUTING [3 1 0 4]

Introduction to Quantum computation, Quantum bits, Single qubit operations, Postulates of quantum mechanics, Quantum Measurement, Bell states, EPR Paradox, No Cloning Theorem, Quantum Gates, Single qubit gates, Pauli Gates, Hadamard gate, Quantum Circuits, Multi-qubit gates, CNOT gate, Toffoli Gate, Fredkin Gate, Universal quantum gates, Quantum Key Distribution, Superdense coding and Quantum Teleportation, Quantum Parallelism and entanglement, The quantum Fourier transform (QFT), Walsh-Hadamard transformation, Quantum search algorithms, Grover’s Search Algorithm, Deutsch Algorithm, Deutsch-Jozsa Algorithm, Bernstein-Vazirani Algorithm, Simon’s Algorithm, Shor’s Factorization algorithm, Quantum error correcting codes. Overview of Qiskit-

IBM quantum computing open-source tool, Designing quantum circuits and implementing quantum algorithms using Qiskit.

References:

1. M. Nakahara and T Ohmi, "Quantum Computing From Linear algebra to Physical Realizations" CRC press 2008.
2. Michael A Nielsen, and Isaac L. Chuang “Quantum Computation & Quantum Information”, (10e), Cambridge University Press, 2011.
3. Eleanor Rieffel and Wolfgang Polak, “Quantum Computing A Gentle Introduction”, MIT Press, 2011.
4. Eric R. Johnston, Nic Harrigan & Mercedes Gimeno-Segovia, “Programming Quantum Computers”, O’REILLY 2019.
5. F. Benatti, M. Fannes, R. Floreanini, and D. Petritis, “Quantum Information, Computation and Cryptography” Springer, 2010.
6. Mika Hirvensalo, “Quantum Computing”, (2e), Springer-Verlag New York, 2004.
7. Jozef Gruska, “Quantum Computing”, McGraw Hill, 1999.
8. Phillip Kaye, Raymond Laflamme and Michele Mosca, “An Introduction to Quantum Computing”, Qxford University Press, 2006.

Course Outcomes:

After completing the course, the student will be able to:

1. Analyse quantum model of computation.
2. Design quantum algorithms.
3. Illustrate quantum protocols such as QKD, Quantum Teleportation and Super Dense Coding.
4. Implement quantum algorithms using Qiskit quantum computing open source tool.
5. Demonstrate various applications of quantum computing.

CSE XXXX: SOFTWARE PROJECT MANAGEMENT [4 0 0 4]

Importance of Software Project Management, Management Principles, Strategic Program Management, Stepwise Project Planning. Project Schedules, Critical Path (CRM) Method, Risk Identification, Cost Schedules. Framework for Management and Control, Collection of Data Project Termination, Managing People, Organizational Behavior, Decision Making, Team Structures, Communication Plans, Case study. Need for Software Quality, Software Quality Assurance, Software Quality factors, Software Development methods, Quality Assurance

Activities, Software Maintenance Quality, and Project Management. Staff Training and Certification Corrective and Preventive Actions, Project Process Control, Computerized Tools, Software Quality Metrics, Limitations of Software Metrics, Cost of Software Quality, Classical Quality Cost Model, Extended Model, Application of Cost Model.

References:

1. Bob Hughes, Mike Cotterell and Rajib Mall, “Software Project Management” (5e), Tata McGraw Hill, New Delhi, 2012.
2. Robert K. Wysocki, “Effective Software Project Management” (4e) – Wiley Publication, 2011.
3. Gopalaswamy Ramesh, “Managing Global Software Projects” – McGraw Hill Education (India), Fourteenth Reprint 2013.
4. Rajib Mall, “Fundamentals of Software Engineering” PHI Learning PVT. LTD, 4th Edition, 2014
5. Marcelo Marinho et.al; “A Systematic review of Uncertainties in Software Project Management”, International Journal of Software Engineering & Applications (IJSEA), Vol.5, No.6, November 2014.
6. Daniel Galin, “Software Quality Assurance”, ISBN 0201 70945 7, Pearson Publication, 2009.
7. Alan C. Gillies, “Software Quality: Theory and Management”, International Thomson Computer Press, 1997.

Course Outcomes:

After completing the course, the student will be able to:

1. Understand the basic tenets of Software Quality and its factors and be exposed to Software Quality Assurance (SQA) with its components.
2. Understand how the SQA components be integrated into the Software Project life cycle.
3. Be familiar with the Software Quality Infrastructure and staffing principles.
4. Utilize the concepts in Software Development Life Cycle and demonstrate their capability to adopt high quality standards.
5. Assess the quality of software product.

CSE XXXX: DEEP LEARNING AND APPLICATIONS [3 1 3 5]

Introduction to Deep Learning & Architectures, Machine learning basics, Neural Networks basics, Feed Forward Neural Networks, Machine Learning Vs. Deep Learning, Representation Learning, Width Vs. Depth of Neural Networks. Activation Functions: Linear, Non-Linear, Sigmoid, Tanh, RELU, LRELU, ERELU, SoftMax. Regularization and Optimization for Deep Learning, Convolutional Neural Networks Architectural Overview, Layers, Filters, Parameter sharing, Regularization. Popular CNN Architectures: ResNet, AlexNet. Transfer Learning: Transfer learning Techniques, Variants of CNN: DenseNet, PixelNet. Sequence Modelling: Recurrent and Recursive Nets, Recurrent Neural Networks, Bidirectional RNNs. Encoder-decoder sequence to sequence architectures, BPTT for training RNN, Long Short Term Memory Networks. Auto Encoders, Regularized Autoencoders , stochastic Encoders and Decoders, Contractive Encoders. Deep Generative Models, Deep Belief networks , Boltzmann Machines , Deep Boltzmann Machine , Generative Adversarial Networks. Recent Trends. SDL: Transformer models, Explainable AI, Multimodal deep learning.

Reference Books

1. Ian Goodfellow, Yoshua Bengio and Aaron Courville, " Deep Learning", MIT Press, 2017.
2. Josh Patterson, Adam Gibson "Deep Learning: A Practitioner's Approach", O'Reilly Media, 2017
3. Umberto Michelucci "Applied Deep Learning. A Case-based Approach to Understanding Deep Neural Networks" Apress, 2018.
4. Kevin P. Murphy "Machine Learning: A Probabilistic Perspective", The MIT Press, 2012.
5. Ethem Alpaydin,"Introduction to Machine Learning", MIT Press, Prentice Hall of India, Third Edition 2014.
6. Giancarlo Zaccone, Md. Rezaul Karim, Ahmed Menshawy "Deep Learning with TensorFlow: Explore neural networks with Python", Packt Publisher, 2017.
7. Antonio Gulli, Sujit Pal "Deep Learning with Keras", Packt Publishers, 2017. 8. Francois Chollet "Deep Learning with Python", Manning Publications, 2017.
8. Rothman, Denis. Transformers for Natural Language Processing: Build innovative deep neural network architectures for NLP with Python, PyTorch, TensorFlow, BERT, RoBERTa, and more. Packt Publishing Ltd, 2021.
9. Samek, Wojciech, Grégoire Montavon, Andrea Vedaldi, Lars Kai Hansen, and Klaus-Robert Müller, eds. Explainable AI: interpreting, explaining and visualizing deep learning. Vol. 11700. Springer Nature, 2019.
10. Multimodal Deep Learning with Tensorflow, by Andrey But, Alexey Miasnikov, Gianluca Ortolani, Packt Publishing Limited, 2019.

Course Outcomes

1. Differentiate the concept of machine learning with deep learning techniques for choosing suitable algorithms for different applications.
2. Understand the concept of CNN and transfer learning techniques to apply it in the classification problems
3. Use RNN for time series prediction.
4. Use autoencoder and deep generative models to solve problems with high dimensional data including text, image, and speech.

5. Design and implement various machine learning algorithms in a range of real-world applications.

CSE XXXX: APPLIED DATA SCIENCE [3 0 0 3]

Python Basics, Understanding Python code, importing modules, Python for statistics and probability: Types of data, importing and visualizing data, basic statistics, probability distributions, Modeling data, Monte Carlo Methods, Matplotlib: visualization charts and plots, covariance, correlation, Predictive Models: Regressions, Machine Learning with Python: Bayesian methods, Naïve classifier, K-Means Clustering, Entropy, Decision Trees, Ensemble Learning. SDL: Data dimensionality reduction techniques, Data Cleaning and normalization, K-Fold validation.

References:

1. Frank Kane, Hands-on Data Science and Python Machine-Learning, Packt Publication, 2017
2. Dirk P. Kroese, Zdravko Botev, Thomas Taimre, Radislav Vaisman, Data Science and Machine Learning: Mathematical and Statistical Methods, CRC Press, 2020
3. Bill Lubanovic, Introducing Python - Modern Computing in Simple Packages, O'Reilly Publication, 2015
4. Allen B. Downey, Think Python-How to think like a computer scientist, (2e) O'Reilly Publication, 2015

Course Outcomes:

After completing the course, the student will be able to:

1. Use Python to automate data analysis
2. Clean and verify the data to ensure it is accurate and uniform
3. Analyze and visualize data to gain insights from data.
4. Comprehend core concepts of machine learning algorithms for regression, clustering, and classification tasks.
5. Apply machine learning concepts to real-world problems using Python.

CSE XXXX: APPLIED NATURAL LANGUAGE PROCESSING [3 0 0 3]

NLP Overview, Word Tokenization, TF-IDF Vectors, Semantic Analysis, Language Processing and Python, accessing text corpora and lexical resources, Processing Raw text, Foundation of

Structured Programming, Doing More with Functions, Program Development, Algorithm Design, A Sample of Python Libraries, Categorization, and Tagging Words, Learning To Classify text, Reasoning with Word2Vec, Real World NLP Challenges – Information Extraction, Question Answering, Dialog Engines. SDL : Long Short Term Memory (LSTM) networks, Sequence to sequence models and attention (Reference: 2)

References:

1. Steven Bird, Ewan Klein and Edward Loper, Natural Language Processing with Python, (1e), O'Reilly Media, 2009.
2. Natural Language Processing in Action, Hobson Lane, Cole Howard, Hannes Max Hapke, Manning, 2019.

Course Outcomes:

After completing the course, the student will be able to:

1. To comprehend python libraries for natural language processing
2. To use popular lexical resources and Python for NLP tasks
3. To extract information from unstructured text and develop methods for text classification
4. To analyze linguistic structures in text
5. To analyze Word2Vec and real-world NLP challenges

CSE **** INTRODUCTION TO DEEP LEARNING [3 0 0 3]

Introduction to neural networks, Humans Versus Computers, Basic Architecture, Training, Common Neural Architectures, Binary and Multiclass Models, Autoencoders, Fundamentals of deep networks, Architectural Principles, Building blocks, Training deep neural networks, Gradient-Descent Strategies, Batch Normalization, Recurrent neural networks (RNN) Architecture, Challenges, Long Short-Term Memory, Gated Recurrent Units, Convolutional neural networks (CNN), Basic Structure, Training a CNN, Advanced topics in deep learning, Generative Adversarial Networks, Applications of deep learning in Risk prediction of diseases, Sentiment Analysis, object detection, audio classification and GAN for Image generation.

References:

1. Charu C Aggarwal, "Neural Networks and Deep Learning", Springer International Publishing, 2018.
2. Josh Patterson and Adam Gibson, "Deep Learning: A Practitioner's Approach", Oreilly, 2018.
3. Ian Goodfellow, Yoshua Bengio, Aaron Courville, "Deep Learning", MIT Press, 2016.

4. H. Sarker, “Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions”, Springer Nature Computer Science, 2(6), 420,2021.

Course Outcomes

After completing the course, the student will be able to:

1. Understand and illustrate different neural network architectures.
2. Analyze and evaluate the training parameters of deep neural networks.
3. Analyze the convolutional and recurrent neural network architectures.
4. Understand the advanced technology of generative adversarial networks.
5. Apply various deep learning techniques to solve real world problems.