NATIONAL ENGINEERING COLLEGE

(An Autonomous Institution Affiliated to Anna University Chennai)

K.R.NAGAR, KOVILPATTI

www.nec.edu.in

DEPARTMENT OF

INFORMATION TECHNOLOGY

REGULATIONS – 2023

CURRICULUM & SYLLABUS OF

M. TECH. INFORMATION AND CYBER WARFARE

REGULATIONS 2023

CURRICULUM AND SYLLABUS

SEMESTER – I

S. No	Course Code	Course Title	Category	Periods Per Week				Total Contact Periods	Credits
				L	T	P	E		
Theory Courses									
1.	23IC11C	Mathematics for Cyber Security	SFC	3	1	0	0	4	4
2.	23IC12C	Research Methodology and IPR	PCC	2	0	0	0	2	2
3.	23IC13C	Introduction to Cyber Warfare	PCC	3	0	0	0	3	3
4.	23IC14C	Advanced Data Structures	PCC	3	1	0	0	4	4
5.	23IC15C	Advanced Network Security	PCC	3	0	0	0	3	3
6.		Elective – I	PEC	3	0	0	0	3	3
7.		Audit Course – I	AC	0	0	0	0	0	0
Practical Courses									
8.	23IC16C	Advanced Data Structures Laboratory	PCC	0	0	2	2	4	2
9.		Laboratory (Based on Electives)	PEC	0	0	4	0	4	2
							TOTAL	**27**	**23**

SEMESTER – II

S. No	Course Code	Course Title	Category	Periods Per Week				Total Contact Periods	Credits
				L	T	P	E		
Theory Courses									
1.	23IC21C	Cyber Attacks Detection and Prevention System	PCC	3	0	0	0	3	3
2.	23IC22C	Internet of Things	PCC	3	0	0	0	3	3
3.	23IC23C	Applied Cryptography	PCC	3	1	0	0	4	4
4.	23IC24C	Cloud Security and Privacy	PCC	3	1	0	0	4	4
5.		Elective – II	PEC	3	0	0	0	3	3
6.		Audit Course – II	AC	0	0	0	0	0	0
Practical Courses									
7.	23IC25C	Mini Project with Seminar	EEC	0	0	2	0	2	1
8.	23IC26C	Cloud Security Laboratory	PCC	0	0	4	0	4	2
9.		Laboratory (Based on Electives)	PEC	0	0	4	0	4	2
							TOTAL	**27**	**22**

SEMESTER – III

S. No	Course Code	Course Title	Category	Periods Per Week				Total Contact Periods	Credits
				L	T	P	E		
Theory Courses									
1.		Elective – III	PEC	3	0	0	0	3	3
2.		Elective –IV	PEC	3	0	0	0	3	3
3.		Elective – V	PEC	3	0	0	0	3	3
4.		Elective – VI	OEC	3	0	0	0	3	3
Practical Courses									
5.	23IC31C	Project Work – I	EEC	0	0	0	12	12	6
						TOTAL		**24**	**18**

SEMESTER – IV

S. No	Course Code	Course Title	Category	Periods Per Week				Total Contact Periods	Credits
				L	T	P	E		
Practical Courses									
1.	23IC41C	Project Work – II	EEC	0	0	0	24	24	12
						TOTAL		**24**	**12**

Total Number of credits: 75

PROGRAMME ELECTIVE COURSES

S. No	Course Code	Course Title	Category	L	T	P	E	C
1.	23IC01E	Security and Privacy in IOT	PEC	3	0	0	0	3
2.	23IC02E	Operations Research	PEC	3	0	0	0	3
3.	23IC03E	Information Ethics for Computer Professionals	PEC	3	0	0	0	3
4.	23IC04E	Cyber Crime and laws	PEC	3	0	0	0	3
5.	23IC05E	Secure Coding Practices	PEC	3	0	0	0	3
6.	23IC06E	Social Network Security	PEC	3	0	0	0	3
7.	23IC07E	Block Chain Technologies	PEC	3	0	0	0	3
8.	23IC08E	IOT Security	PEC	3	0	0	0	3
9.	23IC09E	Android Security	PEC	3	0	0	0	3
10.	23IC10E	Security in Software Defined Networking	PEC	3	0	0	0	3
11.	23IC11E	Biometric Security Analysis	PEC	3	0	0	0	3
12.	23IC12E	Malware Analysis	PEC	3	0	0	0	3
13.	23IC13E	Web Application Security	PEC	3	0	0	0	3
14.	23IC14E	Multimedia Security	PEC	3	0	0	0	3

S. No	Course Code	Course Title	Category	L	T	P	E	C
15.	23IC15E	Enterprise Cyber Security	PEC	3	0	0	0	3
16.	23IC16E	Distributed System Security	PEC	3	0	0	0	3
17.	23IC17E	E – Commerce Security	PEC	3	0	0	0	3
18.	23IC18E	Operating Systems Security	PEC	3	0	0	0	3
19.	23IC19E	Social Network Security Laboratory	PEC	0	0	4	0	2
20.	23IC20E	Android Security Laboratory	PEC	0	0	4	0	2
21.	23IC21E	Principles of Digital Forensics	PEC	3	0	0	0	3
22.	23IC22E	Penetration Testing and Vulnerability Assessment	PEC	3	0	0	0	3
23.	23IC23E	Cyber Warfare in Intelligence and Military operations	PEC	3	0	0	0	3
24.	23IC24E	Cyber Security and Ethical Hacking	PEC	3	0	0	0	3
25.	23IC25E	Forensics Audio and Video Analysis	PEC	3	0	0	0	3
26.	23IC26E	Mobile Device Forensics	PEC	3	0	0	0	3
27.	23IC27E	Cyber Security and Ethical Hacking Laboratory	PEC	0	0	4	0	2
28.	23IC28E	Penetration Testing and Vulnerability Assessment Laboratory	PEC	0	0	4	0	2
29.	23IC29E	Malware Analysis Laboratory	PEC	0	0	4	0	2
30.	23IC30E	Web Application Security Laboratory	PEC	0	0	4	0	2
31.	23IC31E	Multimedia Security Laboratory	PEC	0	0	4	0	2

Audit Courses 1 & 2

S. No	Course Code	Course Title	Course Category	L	T	P	E	C
1.	23AC01E	Technical Report Writing	AC	2	0	0	0	0
2.	23AC02E	Disaster Management	AC	2	0	0	0	0
3.	23AC03E	Sanskrit for Technical Knowledge	AC	2	0	0	0	0
4.	23AC04E	Value Education	AC	2	0	0	0	0
5.	23AC05E	Constitution of India	AC	2	0	0	0	0
6.	23AC06E	Pedagogy Studies	AC	2	0	0	0	0
7.	23AC07E	Stress Management by Yoga	AC	2	0	0	0	0
8.	23AC08E	Personality Development through Life Enlightenment Skills.	AC	2	0	0	0	0

23IC11C MATHEMATICS FOR CYBER SECURITY L T P C
3 1 0 4

Apply the knowledge of linear algebra concepts in data processing

COURSE OUTCOMES

Upon completing the course, the students will be able to:

CO1: interpret group theory concepts in various cryptographic protocols
CO2: analyze the concepts of algebraic structures in network security.
CO3: apply the number theory concepts in network security
CO4: apply the concepts of probability and statistics in encrypted system
CO5: illustrate various pseudorandom numbers generation used for designing security protocols and for its analysis.

GROUP, RINGS AND FIELDS 9 + 3

Groups – Subgroup - Cyclic and Abelian group - Group homomorphism - Permutation groups – Cosets - Primitive roots – Rings - Sub rings, ideals and quotient rings, Integral domains - Rings of polynomials, factorization of polynomials over a field. Fields – Finite fields – GF (pn), GF(2n) - Classification – Structure of finite fields.

VECTOR AND MATRIX NORM 9 + 3

Vector Space - Basis – Dimensions –Inner product –Norm - Systems of Linear Equations- Solving Systems of Linear Equations - Linear Independence - Linear Mappings - Affine Spaces- case study : Least square approximation.

NUMBER THEORY 9 + 3

Introduction - Divisibility - Greatest common divisor - Prime numbers – Fundamental theorem of arithmetic – Mersenne primes - Fermat numbers - Euclidean algorithm - Fermat's theorem Euler totient function - Euler's theorem - Congruences: Definition - Basic properties of congruences - Residue classes - Chinese remainder theorem. Modular Arithmetic and Caesar cipher, quadratic residues.

PROBABILITY AND STATISTICS 9 + 3

Concepts of Probability - Baye's Theorem- , Random Variables- discrete and continuous, central Limit Theorem, Stochastic Process, Markov Chain, Family of random variables – types, densities and distributions, Application of probability in encryption, Statistical inference – Testing of hypothesis.

RANDOM NUMBERS 9 + 3

Pseudorandom number generation: Introduction and examples – Indistinguishability of Probability Distributions - Next Bit Predictors - The Blum-Blum-Shub Generator – Security of the BBS Generator

L: 45; T: 15; TOTAL: 60 PERIODS

REFERENCES

1. Joseph A. Gallian , "Contemporary Abstract Algebra", Cengage Learning 10th Edition , 2021.
2. S.B.Malik, "Basic Number Theory", 2nd Edition, Vikas Publishers, 2018.
3. Leigh Metcalf, William Casey, "Cyber security and Applied Mathematics", Syngress Publisher, 1st Edition, 2016.
4. Chuck Easttom, "Modern Cryptography: Applied Mathematics for Encryption and Information Security", McGraw-Hill Education, 2nd Edition, 2016.
5. Richard Bronson "Schaum's Outline Theory and Problem of Matrix Operations", 2nd Edition, Tata Mc-Graw Hill, 2018.

23IC12C RESEARCH METHODOLOGY AND IPR **L T P C**
2 0 0 2

COURSE OUTCOMES

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

CO1: Understand research problem formulation.
CO2: Analyze research related information.
CO3: Understand the research ethics.
CO4: Understand when IPR would take such important place in growth of individuals & Nation.
CO5: Recognize the importance of Report writing.

RESEARCH FORMULATION AND DESIGN **6**

Defining and formulating the research problem, selecting the problem, necessity of defining the problem, importance of literature review in defining a problem, literature review - primary and secondary sources, reviews, monographs, patents, research databases, web as a source, searching the web, critical literature review, identifying gap areas from literature and research databases, development of working hypothesis – Case study

DATA COLLECTION AND ANALYSIS **6**

Method validation, observation and collection of data, methods of data collection, sampling methods, data processing and analysis strategies and tools, data analysis with statistical packages (SigmaSTAT, SPSS for student t-test, ANOVA, etc.), hypothesis testing – Data Mining (case studies)

RESEARCH ETHICS, IPR AND SCHOLARY PUBLISHING **6**

Ethics - ethical issues, ethical committees (human and animal); IPR- intellectual property rights and patent law, commercialization, copyright, royalty, trade related aspects of intellectual Property rights (TRIPS); scholarly publishing - IMRAD concept and design of research papers; citation and acknowledgement, plagiarism, reproducibility; and accountability

CONTEMPORARY ISSUES IN IPR **6**

Interface between IPR and Human Rights -Interface between IPR and Competition Law -IPR and sustainable development – Impact of Internet on IPR - IPR of Biological systems & E-Commerce.

INTERPRETATION AND REPORT WRITING **6**

Meaning of Interpretation, Technique of Interpretation, Precaution in Interpretation, Significance of Report Writing, Different Steps in Writing Report, Layout of the Research Report, Types of Reports, Oral Presentation, Mechanics of Writing a Research Report, Precautions for Writing Research Reports.

L: 30; TOTAL: 30 PERIODS

REFERENCES

1. Garg, B.L., Karadia, R., Agarwal, F. and Agarwal, U.K., An introduction to Research Methodology-Ⅱ, RBSA Publishers, 2015
2. Kothari, C.R., Research Methodology: Methods and Techniques‖, New Age International, 2018 (Unit 1, Unit 2, Unit 5).
3. Wadehra, B.L. Law relating to patents, trademarks, copyright designs and geographical indications‖. Universal Law Publishing, Reprint, 2011. (Unit 3, Unit 4)
4. Anthony, M., Graziano, A.M. and Raulin, M.L. Research Methods: A Process of Inquiry, Allyn and Bacon 2012.
5. Carlos, C.M., Intellectual property rights, the WTO and developing countries: the TRIPS agreement and policy options. Zed Books, New York, 2000.

23IC13C INTRODUCTION TO CYBER WARFARE L T P C
3 0 0 3

COURSE OUTCOMES

CO1: Compare several cyber attacks using open source intelligence and analyze the attack vectors that were implemented in each.

CO2: Compare the motivations behind cyber warfare and cyber terrorist attacks against corporate and government systems.

CO3: Select the appropriate computer security tools to detect and analyze indicators of an attack.

CO4: Analyze the differences between a cyber warfare attack and a typical malware/virus attack.

CO5: Design a mock scenario that simulates a cyber attack using current attack vectors to prepare for a cyber event.

INTRODUCTION **9**

Introduction to Cyberwarfare - Modes of Attacks - Actors of Cyberwarfare - Types of the Attacks - Motivations of the Actors - Cyberwarfare and International Conflicts - Future Battles: Threats to Critical Infrastructure - Internet Censorship

INTRODUCTION TO CYBERCRIME **9**

Introduction to Cybercrime and Fundamental Issues - Evolution and Types of Cybercrime - Actors of Cybercrime - Understanding Motivated Behavior - Motives for Hacking - Cyber Attacks in a Global Context

INTERNET GOVERNANCE **9**

Internet Infrastructure - Domain Name System - Internet Governance - Importance of Internet Governance - Current Issues in Internet Governance

CYBERWARFARE AND INTERNATIONAL LAW **9**

Principles of Just War - Law of Neutrality and Humanitarian Law - Ambiguity and Attribution - International Treaties - Characteristics of Confidence Building Measures

CYBER SECURITY TOOLS **9**

Penetration testing tools - Password auditing and packet sniffers tools - tools for network defense- Tools for scanning web vulnerabilities - Encryption cybersecurity tools - Tools for monitoring network security - tools for detecting network intrusions

L : 45, TOTAL : 45 PERIODS

REFERENCES

1. Paulo Shakarian, Jana Shakarian, Andrew Ruef, “Introduction to Cyber Warfare - A Multidisciplinary Approach,” First Edition, Syngress (Elsevier), 2019.
2. Jeffrey Carr, “Inside Cyber Warfare,” Second Edition, O’Reilly Media, 2019.
3. Lech J. Janczewski, Lech J. Janczewski, Andrew M. Colarik, “Cyber warfare and cyber terrorism,” First Edition, Information Science Reference, 2019.
4. Michael Erbschloe, John Vacca, “Information Warfare: How to Survive Cyber Attacks,” McGraw-Hill, 2019.
5. Steve Winterfeld, Jason Andress, “The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice,” Syngress, 2019.
6. Paul Rosenzweig, “Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World,” Praeger, 2019.
7. Sushil Jajodia, Paulo Shakarian, V.S. Subrahmanian, Vipin Swarup, Cliff Wang, “Cyber Warfare: Building the Scientific Foundation,” Springer, 2022.

23IC14C **ADVANCED DATA STRUCTURES** **L T P C**
(Common to M.E CSE and M.Tech ICW Programmes) **3 1 0 4**

COURSE OUTCOMES

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

CO1: apply hashing techniques to efficiently store and retrieve data in dictionaries.
CO2: implement heap data structures and skip lists for optimization problems.
CO3: implement algorithms for red-black trees, B-trees and Splay trees.
CO4: implement ontology-based graphs to solve different real-time problems.
CO5: apply suitable data structures for computational geometry problems.

CO1: Apply hashing techniques to efficiently store and retrieve data in dictionaries **12**

Hashing: Hash Function, Collision Resolution Techniques in Hashing, Separate Chaining, Open Addressing, Linear Probing, Quadratic Probing, Double Hashing, Rehashing, Extendible Hashing, Recent Trends in Hashing. **Dictionaries:** Dictionary Abstract Data Type, Hash tables for dictionary - Implementation of Dictionaries – Tries

CO2: Implement heap data structures and skip lists for optimization problems **12**

Heaps: d-Heaps - Leftist Heaps - Binomial Heaps - Fibonacci Heaps - Pairing Heaps-Binomial Queue-Priority Queue. **Skip Lists:** Need for Randomizing Data Structures and Algorithms, Search and Update Operations on Skip Lists, Probabilistic Analysis of Skip Lists, Deterministic Skip Lists

CO3: implement algorithms for red-black trees, B-trees and Splay trees **12**

Trees: Red Black Trees, Splay Trees 2-3-4 Trees, Suffix Trees and Suffix Arrays, Geometric data structures: Quad Trees and Octrees, Treaps, Range query data structure: Priority Range Trees, k-D Trees

CO4: implement ontology-based graphs to solve different real-time problems **12**

Text Processing: Strongly Connected Components - Kosaraju's Algorithm- Network Flows - Edmonds-Karp Algorithm - Planar Graphs - Randomized Minimum Spanning Tree - Graph Traversal on Ontology Based Graphs - Graph Traversal on Ontology-Based Graphs - Ontology-Based Metadata Management

CO5: apply suitable data structures for computational geometry problems **12**

Computational Geometry: Geometric Optimization: closest pair of points, farthest pair of points - Binary Space Partitioning (BSP) Tree - Convex Hull Data Structures - Computational Geometry in Higher Dimensions - Algorithms for higher-dimensional geometric problems: d-D Voronoi diagrams, Delaunay triangulations.

L: 45; T:15; TOTAL: 60 PERIODS

REFERENCES

1. Anchit Bijalwa, “Network Forensics Privacy and Security”, 1st Edition, Taylor & Francis, CRC Press, 2022.
2. Bill Nelson, Amelia Phillips, Christopher Steuart, “Guide to Computer Forensics and Investigations”, 6th Edition, 2019.
3. John Peterson, “Data Structures and Algorithms in Java: A Comprehensive Guide”, Kindle Edition, 2023.
4. G.A.Vijayalakshmi Pai, “A Textbook of Data Structures & Algorithms, Volume 3”, Wiley, 2023.
5. Debasish Ray Chawdhuri, “Java 9 Data Structures and Algorithms”, Packet Publishing, 2017.
6. Yashavant Kanetkar, “Data Structures Through C++”, 3rd Edition, 2019.

23IC15C **ADVANCED NETWORK SECURITY** **L T P C**
3 0 0 3

COURSE OUTCOMES

CO1: Understand and explore the overall concepts of Network security.
CO2: Examine the issues and challenges in network security.
CO3: Apply the recent tools for preventing network security attacks.
CO4: Evaluate security mechanisms using rigorous approaches
CO5: Evaluate network security threats and counter measures.

OVERVIEW OF NETWORK SECURITY **12**

Introduction to network security – Types of network security - Wireless network security – Information security – Cloud Security – Web application security.

NETWORK ATTACKS AND NETWORK SECURITY THREATS **11**

Unauthorized access - Distributed Denial of Service (DDoS) attacks - Man in the middle attacks - Code and SQL injection attacks - Privilege escalation - Insider threats.

RECENT TECHNOLOGIES IN PREVENTING NETWORK SECURITY ATTACKS **11**

Extended Detection and Response (XDR) - Zero Trust Network Access (ZTNA) - Secure Access Service Edge (SASE). Firewall/NGFW- Intrusion Prevention Systems (IPS) - Data Loss Prevention (DLP) - Distributed denial-of-service (DDoS) Protection - Secure Web Gateway (SWG).

RECENT TOOLS IN NETWORK SECURITY **11**

Wire Shark – Snort - Kali Linux - Spy Sweeper – OWASP

L : 45, TOTAL : 45 PERIODS

REFEERNCES

1. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security: Private Communication in a public world”, Third Edition, Prentice Hall, 2022.
2. Eric Rescoria, “SSL and TLS: Designing and Building Secure Systems”, Addison-Wesley Professional, 2020.
3. Jonathan Katz, Yahuda Lindell, Introduction to Modern Cryptography, Third Edition, CRC Press, 2021.
4. Larry L.Peterson, Bruce S. Davie, Computer Networks: A Systems Approach, Sixth Edition, Morgan Kaufmann, 2021.
5. Jon Ericson, Hacking: The Art of Exploitation, Second Edition, No Starch Press, 2010.

23IC16C **ADVANCED DATA STRUCTURES LABORATORY** **L T P E C**
(Common to M.E CSE and M.Tech ICW Programmes) **0 0 2 2 2**

COURSE OUTCOMES

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

CO1: Implement applications based on the concept of heap, skip list and hashing techniques.
CO2: Develop programs for red-black trees, B-trees, AVL and Binary Search trees.
CO3: Develop algorithms for text processing applications.
CO4: Identify suitable data structures and develop algorithms for computational geometry problems

List of Lab Experiment

1. Imagine you are designing a contact management system for a large corporation. The system should allow employees to quickly search for contact information based on the employee's ID number. The system should support the following operations:
    a. Insert: Add a new employee's contact information, including their ID number, name, email, and phone number, into the dictionary.
    b. Retrieve: Given an employee's ID number, retrieve their contact information from the dictionary.
    c. Update: Given an employee's ID number, update their contact information in the dictionary.
    d. Delete: Given an employee's ID number, remove their contact information from the dictionary.
2. Consider the following elements and perform Extendible Hashing: 16,4,6,22,24,10,31,7,9,20,26. Bucket Size: 3 (Assume). Hash Function: Suppose the global depth is X. Then the Hash Function returns X LSBs.
3. With Tries data structures, develop a program that can be used in the web browser to auto complete the text or show many possibilities of the text the user is trying to write.
4. Read the marks obtained by students of second year in an online examination of particular subject. Find out maximum and minimum marks obtained in that subject. Use heap data structure.
5. For a given set of elements (3 6 7 9 12 17 19 21 25 26) create skip list. Find the element in the set that is closest to some given value.
    a. Implement the random_level() function to generate a random level for each inserted node.
    b. Modify the insert() function to handle duplicates. Allow multiple nodes with the same value to be inserted.
    c. Add a function get_level_counts() that returns the number of nodes at each level of the Skip List.
    d. Implement the search() function to find a specific value in the Skip List.
    e. Add a function count_occurrences(value) that returns the number of occurrences of a given value in the Skip List.
    f. Implement the delete() function to remove a specific value from the Skip List.
    g. Add a function remove_duplicates() that removes all duplicate values from the Skip List.
    h. Implement a function get_min() that returns the minimum value in the Skip List.
    i. Implement a function get_max() that returns the maximum value in the Skip List.
    j. Add a function get_range(start, end) that returns a list of values between a given start and end range.
6. Implement the Insertion, count the number of nodes, Search, Clear Tree, Traversal operations in the Red-Black Tree.
7. You are supposed to build a Social Cop in your smartphone. Social Cop helps people report crimes to the nearest police station in real-time. Use k-d tree to search for the police station nearest to the crime location before attempting to report anything by constructing a 2 dimensional k-d tree from the locations of all the police stations in your city, and then querying the k-d tree to find the nearest police station to any given location in the city.
8. Implement the Edmonds-Karp algorithm for finding the maximum flow in a network.
9. Implement Randomized Minimum Spanning Tree

10. Binary Space Partitioning (BSP) Tree
11. Implement a data structure to represent Delaunay triangulations in d-Dimensional space.
12. Implement an algorithm to compute the Voronoi diagram from the Delaunay triangulation.

Mini Projects

1. Web Browser History
2. Tree Visualization and Manipulation
3. Pattern Matching and Text Indexing
4. Dynamic Graph Connectivity
5. Priority range tree
6. Cash Flow Minimiser (Graphs/Multisets/Heaps)
7. File Zipper(Greedy Huffman Encoder)
8. Data Clustering and Pattern Recognition with d-Dimensional Voronoi Diagrams and
9. Delaunay Triangulation.

P: 45; TOTAL: 45 PERIODS

23IC21C CYBER ATTACKS DETECTION AND PREVENTION SYSTEM L T P C
3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: explore modern concepts related to intrusion detection system.
CO2: compare and determine the best approach to reduce the intrusion through quantitative analysis.
CO3: identify and explain the key components of IDS and IPS.
CO4: explore the principles and techniques of fusing diverse sources of security data.
CO5: apply wireless intrusion detection and prevention knowledge and skills to real-world wireless network scenarios and case studies.

INTRODUCTION **8**

Introduction to Intrusion – Need of Intrusion Detection – Classification of Intrusion Detection Systems - Components and Architecture – Source of vulnerabilities – Attacks against various Security Objectives – Countermeasures of attacks.

INTRUSION DETECTION AND PREVENTION TECHNOLOGIES **10**

Host Based IDS – Network Based IDS – Information Source for IDS – Host and Network vulnerabilities and countermeasures – Intrusion detection techniques, misuse detection: pattern matching, rule based and state-based anomaly detection: Statistical based, machine learning based, data mining-based hybrid detection.

IDS AND IPS ARCHITECTURE **10**

Tiered architecture: Single-tiered, multi-tiered, peer-to-peer – Sensor: Functions, deployment and security – Agent: Functions, deployment and security, Manager component: Functions, deployment and security – Information flow in IDS and IPS – Defending IDS/IPS – Case study on Commercial and open-source IDS.

ALERT MANAGEMENT AND CORRELATION DATA FUSION **8**

Alert correlation – Preprocess – Correlation techniques – post process – Alert correlation Architecture - Cooperative Intrusion Detection - Cooperative discovery of intrusion chain –

abstraction-based intrusion detection – Interest based communication and cooperation – Agent based cooperation

WIRELESS IDPS **9**

Threats against WLANs, 802.11 Wireless Infrastructure Attacks, WEP Attacks, Wireless Client Attacks, Bluetooth Attacks, Cell phones, Personal Digital Assistance and Other Hybrid Devices Attack Detection, Jail breaking - Threat Briefing – Quantifying risk - Return on Investment (ROI).

L: 45, TOTAL: 45 PERIODS

REFERENCES

1. Ali A.Ghorbani, Wei Lu, “Network Intrusion Detection and Prevention: Concepts and Techniques”, First Edition, Springer US, 2019
2. Chris Sanders and Jason Smith, “Applied Network Security Monitoring Collection, Detection, and Analysis”, First Edition, Syngress, 2014.
3. Al-Sakib Khan Pathan, “The State of the Art in Intrusion Prevention and Detection”, First Edition, CRC Press, 2014.
4. Ankit Fadia and Mnu Zacharia, “Intrusion Alert – an ethical hacking guide to intrusion detection”, Second Edition, Vikas Publisher, 2007.
5. Earl Carter, Jonathan Hogue, “Intrusion Prevention Fundamentals”, First Edition, Pearson Education, 2006.

23IC22C **INTERNET OF THINGS** **L T P C**
3 0 0 3

COURSE OUTCOMES

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

CO1: analyze various design methodologies and enabling technologies for Internet of Things platform.
CO2: apply the appropriate model for building things in IoT.
CO3: examine the standard IoT protocols by emphasizing their characteristics and interoperability.
CO4: apply the utilities of ESP32 for implementing diverse IoT applications.
CO5: analyze the applications of IoT in real-time scenarios.

IoT DESIGN METHODOLOGIES **9**

Internet of Things - Physical Design- Logical Design- IoT Enabling Technologies - IoT Levels and Deployment Templates - Domain Specific IoTs - IoT and M2M - IoT System Management with NETCONF-YANG- IoT Platforms Design Methodology.

IoT MODELING **9**

IoT Reference architecture - High-level M2M ETSI architecture - IETF architecture - OGC architecture - Reference models: Domain model - Information model - Functional model - Communication model - Case Studies: Monitoring soil conditions, Smart fridge solutions.

IoT PROTOCOLS **9**

Protocol Standardization for IoT - MQTT - CoAP – AMQP - Zigbee - BLE - 6LowPAN - LoRaWAN- Z-Wave - NarrowBand-IoT.

IoT APPLICATIONS **9**

Role of ESP32 in IoT applications - ESP-IoT Development Framework (IDF) - Architecture and GPIO Programming - Interfacing sensors - Creating a web server - Data Storage - Edge computing with ESP32 - Applications: LED Blinking, Maintaining the distance of Things, Bluetooth communication, Humidity measurement

REAL TIME IoT SYSTEM **9**

Smart lighting - Intrusion detection system - Emergency response - Smart parking - Weather monitoring - Forest fire detection - Smart grid - Inventory management - Smart payment - Smart irrigation - Wearable electronics.

L: 45, TOTAL: 45 PERIODS

REFERENCES

1. Arshdeep Bahga and Vijay Madisetti, “Internet of Things – A Hands-on Approach” Second Edition, Orient Blackswan Private Limited - New Delhi, 2019.
2. Simone Cirani, Gianluigi Ferrari, Marco Picone and Luca Veltri, “Internet of Things: Architectures, Protocols and Standards” First Edition, Wiley, 2018.
3. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton and Jerome Henry, “IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things”, First Edition, Cisco Press, 2017.
4. Vedat Ozan Oner, “Developing IoT Projects with ESP32”, First Edition, Packt Publishing, 2021.
5. Olivier Hersent, David Boswarthick and Omar Elloumi, “The Internet of Things - Key applications and Protocols”, Second Edition, Wiley, 2018.
6. Rajkumar Buyya and Amir Vahid Dastjerdi, "Internet of Things: Principles and Paradigms", Second Edition, Elsevier, 2020.
7. Marco Zappatore, "Internet of Things- Architectures, Protocols and Standards" First Edition, Springer, 2018.

23IC23C **APPLIED CRYPTOGRAPHY** **L T P C**
3 1 0 4

COURSE OUTCOMES

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

CO1: To apply basic mathematical concepts and number theory in cryptography.
CO2: To acquire the knowledge of providing security using symmetric encryption.
CO3: To design public key cryptosystems for secure communication.
CO4: To Evaluate security mechanisms using Hash functions.
CO5: To Demonstrate various security applications

MATHEMATICAL FOUNDATION FOR CRYPTOSYSTEM **13**

Computer security Concepts, OSI Security Architecture, Security Mechanisms and Network security Models, Classical Encryption Techniques, Basic Concepts in Number Theory and Finite Fields, Cryptographic Protocols.

BLOCK CIPHERS AND KEY MANAGEMENT TECHNIQUES **11**

Block Ciphers and the Data Encryption Standard, Advanced Encryption Standard, Block Cipher Operation - Lucifer, Madryga, NewDES, FEAL, REDOC, LOKI, Pseudorandom Number

Generation and Stream Ciphers - Hughes XPD/KPD, Nanoteq, Rambutan, Gifford, Cryptographic Key Management Techniques.

PUBLIC KEY CRYPTOGRAPHY **11**

Public Key Cryptography and RSA -Knapsack Algorithms, Pohlig - Hellman, Rabin. Diffie-Hellman Key Exchange, Elgamal Cryptographic System, Elliptic Curve Cryptography, LUC, Finite Automaton Public-Key Cryptosystems, Asymmetric Ciphers

HASH FUNCTIONS AND DIGITAL SIGNATURE **12**

Authentication requirement – Authentication function – MAC – Hash function – Security of Hash function and MAC – MD5 - SHA - HMAC – CMAC - Digital signature and authentication protocols – DSS – EI Gamal – Schnorr - Blind Signatures for unreachable payments, Post Quantum Cryptography, Lattice based post quantum cryptography.

APPLICATIONS OF CRYPTOGRAPHIC ALGORITHMS **13**

IBM Secret-Key Management Protocol, MITRENET, ISDN, STU-III, Kerberos, KryptoKnight, SESAME, IBM Common Cryptographic Architecture, ISO Authentication Framework, Privacy-Enhanced Mail (PEM), Message Security Protocol (MSP), Pretty Good Privacy (PGP), Smart Cards, Universal Electronic Payment System (UEPS), Clipper, Crypto currencies - Bitcoin, Tor (The Onion Router).

L: 45, T:15; TOTAL: 60 PERIODS

REFERENCES

1. William Stallings, “Cryptography and Network Security Principles and practice”, Eighth Edition, Pearson Education, 2020.
2. Bruce Schneier, “Applied Cryptography: Protocols, Algorithms and Source Code in C”, Second Edition, John Wiley and Sons, 2020.
3. Behrouz A. Forouzan and Debdeep Mukhopadhyay, “Cryptography and Network Security”, Third Edition, McGraw-Hill Education, 2015.
4. Jonathan Katz and Yehuda Lindell, “Introduction to Modern Cryptography”, A Chapman and Hall book, Second Edition, CRC Press, USA, 2015.
5. Douglas R. Stinson and Maura Paterson “Cryptography: Theory and Practice”, Fourth Edition, Chapman & Hall/CRC, USA, 2018.
6. Jeffrey Hoffstein, “An Introduction to Mathematical Cryptography”, Springer, USA, 2014.

23IC24C **CLOUD SECURITY AND PRIVACY** **L T P C**
3 1 0 4

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: characterise the different cloud technologies and related architectures.
CO2: identify the threats, risks, vulnerabilities associated with cloud-based applications.
CO3: integrate cryptographic key management into cloud applications and services.
CO4: analyse industry security standards, certificates, audit policies and compliance requirements.
CO5: apply best practices for securing AWS applications and services.

CLOUD COMPUTING ESSENTIALS **12**

Introduction – Characteristics – Cloud Computing models: Infrastructure as a Service –Platform as a Service – Software as a service – Cloud services and technologies – Cloud deployment models - NIST Cloud Reference Model – ITU-T Reference model – Network requirements – Cloud security

– Vulnerabilities and attacks - Cloud security baselines – Threats Infrastructure and Host threat – service provider threat – Genetic threats - Threats assessment.

RISK ANALYSIS AND DIVISION OF RESPONSIBILITY **12**

Risk and Trust Management: Risk analysis, Trust and Management – Cloud risk assessment – Risk and Trust models for cloud – Risk management framework – Cloud's provider risk management – Cloud consumer's risk management –Cloud SLA – Risk mitigation methods.

ACCESS CONTROL AND CRYPTOGRAPHIC KEY MANAGEMENT **12**

Key management: lifecycle –System design – Drivers for cloud key management design – Key management strategies – Cloud user controls - Access control: Policies - Layers of security needs – Multilevel authentication – encryption – Password management – Secure cloud Architecture.

CLOUD SECURITY STANDARDS AND COMPLIANCE **12**

Negotiating Cloud Security Requirements with Vendors - Managing Legal Compliance Risk - Integrity Assurance for Data Outsourcing - Secure Computation Outsourcing - Trusted Computing Technology - Resolving Cloud Computing Security Problems - Assuring Compliance with Government Certifications.

AMAZON WEB SERVICES AND SECURITY **12**

Introduction – Shared Responsibility Model - Major AWS Security Pillars - Identity and access management – Managing accounts –Policies and procedures for secure access – Virtual private cloud – Protecting data in cloud – logging and audit trails – Continuous monitoring – Incidence response and remediation.

L: 45, T: 15; TOTAL: 60 PERIODS

REFERENCES

1 Naresh Kumar, Sehgal Pramod Chandra, P. Bhatt John M. Acken, "Cloud Computing with Security Concepts and Practices", Second Edition, Springer International Publisher, 2020.
2 Tim Mather, Subra Kumaraswamy and Shahed Lati, "Cloud Security and Privacy", First Edition, September 2019.
3 John R. Vacca, "Cloud Computing Security: Foundations and Challenges", First Edition, CRC Press, 2017.
4 Dylan Shields, "AWS Security", First Edition, Manning Shelter Island, 2022.
5 Liliana F. B. Soares, Diogo A. B. Fernandes, Joao V. Gomes, Mario M. Freire, "Security, Privacy and Trust in Cloud Systems", First Edition, Springer-Verlag Berlin Heidelberg, 2014.
6 Siani Pearson, George Yee, "Privacy and Security for Cloud Computing", First Edition. Springer-Verlag London, 2013.

23IC26C **CLOUD SECURITY LABORATORY** **L T P C**
0 0 4 2

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: identify security requirements and security risks in cloud environment.
CO2: demonstrate different monitoring and auditing processes for security and privacy in cloud.

List of Experiments

1 Vulnerability Attacks:
- Sending a large volume of DNS queries

2 Risk Analysis:
- Assess risk in a cloud environment

3 Access Control:
- Role-based access control mechanism.
- Attribute-based access control mechanism

4 Password Protection:
- Set up password-protected cloud storage solutions
- Implement password policies for virtual machines (VMs) in the cloud

5 Log and Audit Traits:
- Log monitoring system with incident management in the cloud.
- Simulate log forensics

6 Privacy Protection:
- Implement any encryption algorithm to protect the images.
- Implement any image obfuscation mechanism.
- Implement data anonymization techniques over the simple dataset

Tools Required:
- CloudSimv6.0.0 - beta

P: 30; TOTAL: 30 PERIODS

Course Code	PROJECTWORK-I	L	T	P	E	C
23IC31C		0	0	0	12	6

COURSE OUTCOMES

Upon the successful completion of the course, the student will be able to

Experiential Components

CO1:formulate a problem that pertains to a newly emerging research issue.(PDL2)
CO2:perform literature study with a comparative analysis of the existing approaches.(PDL2)
CO3: devise the novel methodology to address the research gaps and challenges of the identified problem. (PDL2)
CO4:identify the software and hardware requirements for developing the solution.(PDL1)

CO1: formulate a problem that pertains to a newly emerging research issue. E: 45

- Each student individually selects their area of interest and work under the supervision of their allotted guide approved by Head of the department.
- Students can select any topic which is related to engineering design.

CO2: perform literature study with a comparative analysis of the existing approaches. E: 45

- Identify appropriate peer reviewed, SCI indexed journals/Scopus indexed conference articles in the relevant area.
- Carry out literature study based on approaches, dataset, experimental setup, performance analysis metric by considering computational complexity.

CO3: devise the novel methodology to address the research gaps and challenges of the identified problem. **E: 45**

- Explore the research gap and challenges with respect to dataset, experimental setup
- Identify novel methodology that addresses the identified gaps and challenges to enhance the performance.

CO4: identify the software and hardware requirements for developing the solution. **E: 45**

- Recognize the software tools and hardware requirements for implementing the identified problem.
- Students should submit a project report in the standard prescribed format.
- The progress of the project is evaluated based on minimum of three reviews and a final Viva-voce examination.

E: 180;TOTAL: 180 PERIODS

Course Code	PROJECTWORK - II	L	T	P	E	C
23IC41C		0	0	0	24	12

COURSE OUTCOMES

Upon the successful completion of the course, the students will be able to

Experiential Components

CO1: design methodology for identified research problem to address emerging issues. (PDL2)
CO2: develop experimental setup, conduct research and compare the performance with SOTA analysis. (PDL2)
CO3: demonstrate the research outcomes in peer reviewed Journals / Conferences. (PDL2)

Softskill Components

Disseminate the research competency, project management, function as an efficient individual.

Each student individually extends the selected research idea during Project Work - I and work under the supervision of the domain expertise related guide approved by Head of the department. Review Committee will be conducted by the Project Co-ordinator, respective Guide and domain specific reviewers being nominated by the Head of department.

CO1: design novel methodology for identified research problem to address emerging issues

- Review – I, will focus mainly on the critical hypothesis design of methodology for the research problem identified and bring valid conclusion for the appropriateness of novelty in solving the research problem by addressing the research gaps and challenges with the support of investigating the recent related works. **L: 9**

CO2: develop experimental setup, conduct research and compare the performance with SOTA analysis **E:120**

- Based on the domain chosen, appropriate selection of standard experimental data sets and their quality has to be validated. Based on the research method proposed, experimental steps have to be arrived in addition to the various ways of performance metrics that can help to measure the improvement in system modeling. To bring hope for the novel approach, the comparison with State-of-the-art (SOTA) analysis is to be carried out.
- Review – II, will assure the quality of experimental data and conduct of research with originality. The performance metrics will be gauged based on existing research works to analyze the SOTA comparisons

CO3: demonstrate the research outcomes in peer reviewed Journals / Conferences.

- Identify appropriate peer reviewed SCI / ESCI / Scopus indexed Journals / Conference avenues, to bring highlights for the successful conduct of project work.
- Review – III, will ensure the plagiarism checks using Grammarly / Turnitin tools and validate the template requirements as per the submission guidelines of the identified Journal / Conference. Overall demonstration of the arrived solution and it's suitability for solving real-time challenges to be verified. **E:150**
- Final Project report of project may include the title, theory/hypothesis, literature review, research gaps & challenges, objectives, materials required, methodology, experimental observations, results and discussions, SOTA analysis, conclusion, future work, and references.

E: 360; TOTAL: 360 PERIODS

Course Code	SECURITY AND PRIVACY IN IOT	L	T	P	E	C
23IC01E		3	0	0	0	3

COURSE OUTCOMES

Upon the successful completion of the course, the student will be able to

Theory Component

CO1: recognize security concerns in IoT applications to ensure business continuity and system integrity

CO2: apply security requirements across various aspects of IoT, ensuring end-to-end security, privacy, and data integrity.

CO3: develop IoT systems that prioritize privacy preservation in various application domains.

CO4: implement access control mechanisms and data encryption to prevent unauthorized access to sensor data.

CO5: apply policy-based approaches to obtain and manage informed consent in IoT systems.

INTRODUCTION: SECURING INTERNET OF THINGS **L:9**

Overview of Security in IoT – Security Requirements in IoT architectures – Security in Enabling Technologies – IoT Security Life Cycle – Cryptographic Fundamentals for IoT Security Engineering - Security Concerns in IoT Applications.

SECURITY ARCHITECTURE IN INTERNET OF THINGS **L: 9**

Insufficient Authentication/Authorization – Insecure Access Control – Threads to Access Control, Privacy, and Availability – Attacks Specific to IoT – Malware Propagation and Control in Internet of Things.

PRIVACY PRESERVATION **L:9**

Privacy Preservation Data Dissemination - Privacy Preservation for IoT used in Smart Building – Exploiting Mobility Social Features for Location Privacy Enhancement in Internet of Vehicles – Lightweight and Robust Schemes for Privacy Protection in Key personal IOT.

TRUST, AUTHENTICATION FOR IOT **L: 9**

Trust and Trust Models for IoT – Emerging Architecture Model for IoT Security and Privacy – preventing Unauthorized Access to Sensor Data – Authentication in IoT – Computational Security for the IoT – Secure Path Generation Scheme for real-Time Green IoT – Security Protocols for IoT Access Networks.

SOCIAL AWARENESS AND APPLICATIONS **L: 9**

User Centric Decentralized Governance Framework for Privacy and Trust in IoT – Policy Based Approach for Informed Consent in IoT - Security and Impact of the IoT on Mobile Networks – Security Concerns in Social IoT – Security for IoT Based Healthcare – Smart cities.

REFERENCES:

1. Lidia Fotia, Fabrizio Messina, Domenico Rosaci, Giuseppe M.L. Sarné," Security, Trust and Privacy Models, and Architectures in IoT Environments", Springer, 2023.
2. Shivani Agarwal, Sandhya Makkar, Duc-Tan Tran," Privacy Vulnerabilities and Data Security Challenges in the IoT" CRC Press, 2020.
3. Shancang Li, Li Da Xu, "Securing the Internet of Things," Syngress (Elsevier)publication, 2017, ISBN: 978-0-12-804458-2.
4. Fei Hu, "Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and

Implementations," CRC Press (Taylor & Francis Group), 2016, ISBN:978-1-4987-23190.
5. Arshdeep Bahga, Vijay Madisetti, "Internet of Things – A Hands-on approach," VPT Publishers, 2014, ISBN: 978-0996025515.
6. Alasdair Gilchris, "Iot Security Issues," Walter de Gruyter GmbH & Co, 2017.
7. Sridipta Misra, Muthucumaru Maheswaran, Salman Hashmi, "Security Challenges and Approaches in Internet of Things," Springer, 2016.
8. Brian Russell, Drew Van Duren, "Practical Internet of Things Security," Packet Publishing Ltd, 2016.

L: 45; TOTAL: 45 PERIODS

Course Code	OPERATIONS RESEARCH	L	T	P	E	C
23IC02E		3	0	0	0	3

COURSE OUTCOMES

Upon the successful completion of the course, the student will be able to

Theory Component

CO1: apply the dynamic programming to solve problems of discrete and continuous variables.
CO2: apply the concept of non-linear programming
CO3: execute sensitivity analysis
CO4: model the real-world problem and simulate it

INTRODUCTION **L:9**

Optimization Techniques- Model Formulation- models, General L.R Formulation- Simplex Technique-Sensitivity Analysis.

LINEAR PROGRAMMING **L: 9**

Formulation of a LPP - Graphical solution revised simplex method - duality theory - dual simplex method - sensitivity analysis - parametric programming-Transportation and Assignment problems.

NONLINEAR PROGRAMMING PROBLEM **L:9**

Nonlinear programming problem - Kuhn-Tucker conditions min cost flow problem - max flow problem - CPM/PERT.

SCHEDULING AND INVENTORY CONTROL MODELS **L: 9**

Scheduling and sequencing - single server and multiple server models - deterministic inventory models - Probabilistic inventory control models - Geometric Programming.

FINITE AND INFINITE QUEUING MODELS **L: 9**

Finite Queuing Models: Introduction, Finite Queuing Models, nfinite Queuing Models: Introduction, Queuing Theory, Operating Characteristics of a Queuing System, Constituents of a Queuing System, Service Facility, Queue Discipline.

REFERENCES:

1. Frederick S. Hillier, Gerald J. Lieberman, Bodhibrata Nag, Preetam Basu, "Introduction to Operations Research", SIE, 11th Edition, 2018.
2. H.A. Taha, Operations Research, An Introduction, PHI, 2008.
3. J.C. Pant, Introduction to Optimisation: Operations Research, Jain Brothers, Delhi, 2008.
4. Hitler Libermann Operations Research: McGraw Hill Pub. 2009.
5. Pannerselvam, Operations Research: Prentice Hall of India 2010.
6. Harvey M Wagner, Principles of Operations Research: Prentice Hall of India 2010.

L: 45; TOTAL: 45 PERIODS

Course Code	INFORMATION ETHICS FOR COMPUTER	L	T	P	E	C
23IC03E	PROFESSIONALS	3	0	0	0	3

COURSE OUTCOMES

Upon the successful completion of the course, the student will be able to

Theory Component

CO1: develop a comprehensive understanding of ethics in business and IT professionals
CO2: analyze strategies for maintaining trustworthy computing environments
CO3: gain knowledge on organizational privacy, threats, attacks and security policies
CO4: identify ethical concerns, and propose strategies for addressing ethical issues
CO5: apply the ethics of Information and Technology in real time applications.

OVERVIEW OF COMPUTER ETHICS **L:9**

Ethics in Business World - Ethical Consideration in Decision Making - Ethics for IT Professionals - Professional Relationships - IT Professional Malpractices - Common Ethical Issues for IT Users – Certification.

ISSUES IN COMPUTER ETHICS **L: 9**

Cybercrime - Security Attacks - Primary Perpetrators - Industrial Spies and Competitive Intelligence - Cybercriminals - Cyber Terrorists - Risk Assessment - Trustworthy Computing.

NETWORKED COMMUNICATIONS **L:9**

Cyber Security - Identification of Theft - Anonymity on Internet - Strategies for Consumer Profiling - Electronic Discovery - Advanced Surveillance Technology - Legal Developments in Cyber Laws - Public Concerns about Security - Preventive Measures.

RESPONSIBILITY ISSUES AND RISK ASSESSMENT **L: 9**

Element of an Ethical Organization - Contingent Worker - Recruitment of Contingent Workers - H-1B Workers - Whistle Blowing – Outsourcing – Case Study on Security Breach.

REGULATORY ISSUES AND CHALLENGES **L: 9**

Impact on Standard of Living and Productivity – Digital Divide and its Factors – Universal Access – Impact on Healthcare costs – Big Data and Cloud – Information and Communication Technology – Telemedicine and Mobility – Electronic Health Record - Case Study on Data Breach.

REFERENCES:

1. G.K. Awari, Sarvesh V Warjurkar, “Ethics in Information Technology”, First Edition, CRC Press, Taylor & Francis, 2022.
2. Jocelyn O.Padallan, “Information and Computer Ethics”, Ebook Edition, Arcler Press, 2020.
3. John T. F. Burgess, Emily J. M. Knox, “Foundations of Information Ethics”, Sixth Edition, Kindle Edition, 2019.
4. Adriano Fabris, “Ethics of Information and Communication Technologies”, First Edition, Springer International Publishing, 2018.

L: 45; TOTAL: 45 PERIODS

Course Code	CYBER CRIME AND LAWS	L	T	P	E	C
23IC04E		3	0	0	0	3

COURSE OUTCOMES

Upon the successful completion of the course, the student will be able to

Theory Component

CO1: Elaborate the types and impacts of cyber crimes and Cyber Terrorism

CO2: Familiarity with international and national legal frameworks

CO3: Evaluate the implications of these laws for business operations and compliance requirements.

CO4: Evaluate various authentication technologies and their applications in ensuring the integrity and authenticity of electronic records.

CO5: Analyze the legal requirements and standards that certifying authorities must comply with to operate.

OVERVIEW OF CYBER CRIME AND CYBER TERRORISM **L:9**

Overview - Classification of Computer Crime - Cyber Terrorism and Information Warfare: Risk and Critical Infrastructure Attacks - Information Attacks - Cyber and Technological Facilitation - Propaganda and Promotion - Cyberterrorism as an Adjunct Attack - Kinds of cyber crimes - Impact of Cyber Crime.

DEFINITIONS UNDER IT ACT, 2000 **L: 9**

Definitions under IT Act, 2000 - Concept of Internet - Web Centric Business - E Business and its significance - Electronic Governance – IT Act : Offences – Security Concerns and Preventive Measures - International Cyber Law Frameworks - National Cyber Crime Laws – Regulatory Bodies and Enforcement Agencies - Cyber jurisdiction.

CONTEMPORARY BUSINESS ISSUES IN CYBER SPACE **L:9**

Security risks - Instant messaging platform - Social networking sites - Mobile applications and Internet of Things (IoT) - Domain name dispute and their resolution - E-forms – E-money - Regulations of PPI (Pre-Payment Instruments) by RBI - Electronic Money Transfer - Privacy of Data and Secure Ways of Operation in Cyber Space.

ELECTRONIC RECORDS **L: 9**

Authentication of Electronic Records - Legal Recognition of Electronic Records – Legal Recognition of Digital Signatures - Applications and usage of electronic records and Digital Signatures in Government and its Agencies - Retention of Electronic Records – Intermediaries and their liabilities - Attribution, Acknowledgement and Dispatch of Electronic Records – Secure Electronic Records and Digital Signatures.

REGULATORY FRAMEWORK **L: 9**

Regulatory Framework Regulation of Certifying Authorities - Appointment and Functions of Controller - License to issue Digital Signatures Certificate - Renewal of License - Controller's Powers - Procedure to be Followed by Certifying Authority - Issue, Suspension and Revocation of Digital Signatures Certificate - Duties of Subscribers - Penalties and Adjudication – Appellate Tribunal – Offences - Overview of GDPR and Indian data protection regime.

REFERENCES:

1. Robert W. Taylor, Eric J. Fritsch, Michael R. Saylor, William L. Tafoya, "Cyber Crime and Cyber Terrorism", 4th Edition, Pearson, 2021.
2. Brian Craig, "Cyberlaw: The Law of the Internet and Information Technology, 1st Edition, Pearson, 2021.
3. Nisha Dhanraj Dewani, Zubair Ahmed Khan, Aarushi Agarwal, Mamta Sharma, Shaharyar Asaf Khan, "Handbook of Research on Cyber Law, Data Protection, and Privacy", IGI Global, 2022.
4. Schreider Tari, "Cybersecurity Law, Standards and Regulations," 2nd Edition, 2020.

5. Jeff Kosseff, "Cybersecurity Law," 3rd Edition, Wiley, 2022.
6. Jay Kesan, Carol Hayes, "Cybersecurity and Privacy Law in a Nutshell", 1st Edition, West Academic Publishing, 2019.
7. Marjie Britz, Computer Forensics and Cyber Crime - An Introduction, Pearson, 2013.

L: 45; TOTAL: 45 PERIODS

Course Code	SECURE CODING PRACTICES	L	T	P	E	C
23IC05E		3	0	0	0	3

COURSE OUTCOMES

Upon the successful completion of the course, the student will be able to

Theory Component

CO1: inscribe the need for secure coding and proactive development process.

CO2: demonstrate secure coding practices in programming languages.

CO3: enumerate input issues related to database and web.

CO4: analyse the impact of principles of software security engineering.

INTRODUCTION **L:9**

Need for secure systems- Proactive security development process - Security principles to live by threat modeling.

SECURE CODING IN C **L: 9**

Character strings- String manipulation errors – String Vulnerabilities and exploits – Mitigation strategies for strings- Pointers – Mitigation strategies in pointerbased vulnerabilities – BufferOverflow based vulnerabilities.

SECURE CODING IN C++ AND JAVA **L:9**

Dynamic memory management- Common errors in dynamic memory management- Memory managers- Double –free vulnerabilities –Integer security- Mitigation strategies.

DATABASE AND WEB SPECIFIC INPUT ISSUES **L: 9**

Introduction to Input Validation – Use of stored procedures- Building SQL statements securely- XSS related attacks and remedies.

SOFTWARE SECURITY ENGINEERING **L: 9**

Requirements engineering for secure software: Misuse and abuse cases- SQUARE process model- Software security practices and knowledge for architecture and design.

REFERENCES:

1. Michael Howard, David LeBlanc, "Writing Secure Code", Microsoft Press, Second Edition, 2003.
2. Robert C.Seacord, "Secure Coding in C and C++", Pearson Education, Second Edition, 2013.
3. Julia H. Allen, Sean J. Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead, "Software Security Engineering: A guide for Project Managers", Addison-Wesley Professional, 2008.

L: 45; TOTAL: 45 PERIODS

23IC06E SOCIAL NETWORK SECURITY L T P C
3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: inscribe complex dynamics and defenses against online threats in secure digital communities.
CO2: synthesize trust management policies in social networks.
CO3: examine the intricate access control mechanisms and applications
CO4: explore identity management strategies in social media.
CO5: analyze various privacy preservation practices in social networks

ONLINE SOCIAL NETWORKS AND SECURITY ISSUES 9

Introduction to Social Networks - The Meaning of Community –From offline to online Communities - Evolution of Online Social Networks –analysis and Properties - Trust Management – Controlled Information Sharing – Identity Management – Privacy Threats and Defenses – Terrorism Threats and Defenses.

TRUST MANAGEMENT 9

Trust, Policies and Reputation Systems – Trust properties – Trust Components – Social trust and Social Capital – Trust Evaluation Model- recognizing digital friends – Case study: Buying a used car – An Experiment.

ACCESS CONTROL MECHANISMS 9

Access control in Data Management System – Access control Models – Privacy settings in Commercial Online Social Networks – Existing Access control approaches. User managed access control in web based social networks, social semantic network based access control. Case Study: Avatar Facial Biometric authentication using wavelet Local Binary Patterns.

IDENTITY MANAGEMENT 9

Digital Identity – Identity Management Models – Self-Presentation – Identity Disclosure – Identity Theft. Case Study: An analysis of Anonymity in the Bitcoin system.

PRIVACY PRESERVATION 9

Supporting data privacy in P2P Systems – Encryption for Peer to Peer Social Networks - Privacy preserving reputation management in social networks – security and privacy issues in mobile social networks.

L: 45; TOTAL: 45 PERIODS

REFERENCES

1. Barbara Carminati, Elena Ferrari, Marco Viviani, “Security and Trust in Online Social Networks”, Springer International Publisher, 2022.
2. Richard Chbeir, Bechara Al Bouna, “Security and Privacy Preserving in Social Networks”, Springer- Verlag Veinna, 2016.
3. Yaniv Altshuler, Yuval Elovici, Armin. B.Cremers, Nadav Aharony, Alex Pentland, “Security and Privacy in Social Networks”, Springer New York, 2014.
4. Vincent Buskens, “Social Networks and Trust”, Springer, 2014.

Course Code	BLOCKCHAIN TECHNOLOGIES	L	T	P	E	C
23IC07E		3	0	0	0	3

COURSE OUTCOMES

Upon the successful completion of the course, the student will be able to

Theory Component

CO1: identify the core principles and components of blockchain technology.

CO2: demonstrate the foundational concepts of blockchain technology, including decentralized ledgers, cryptographic principles, and consensus mechanisms.

CO3: apply analytical skills to identify and evaluate real-world use cases where blockchain technology can be effectively applied across various industries.

CO4: compare and contrast between different blockchain platforms, such as Ethereum and Hyperledger, in terms of their features, benefits, and suitability for specific use cases.

CO5: develop practical competencies in designing, coding, and deploying smart contracts.

INTRODUCTION AND ESSENTIALS OF BLOCKCHAIN **L:9**

Overview of Blockchain– Blockchain types – Blockchain Framework – Block structure – Scaling Blockchain – Essentials - Cryptography primitives – Hash Functions – Secure Hash Algorithm (SHA) – Public key cryptography – Merkle Tree.

Case Study: Blockchain – The Technology for Document Management

BITCOIN **L: 9**

History – Wallets – Digital keys and Addresses – Addresses in Bitcoin – Transaction – Digital Signature – Mining and Consensus in Bitcoin – Forking. Case Study: Blockchain in the Insurance Industry.

ETHEREUM BLOCKCHAIN **L:9**

Overview – History – Smart Contracts- Challenges in implementing Smart contracts – Ethereum Development Tools – Ethereum Transactions – Gas and Transaction fees – Mist Browser. Case Study: India's Income Tax Department's simplification of Tax Procedures.

HYPERLEDGER **L:9**

Introduction – Architecture – Community and Development – Hyperledger Smart Contracts – The Functioning of Hyperledger - Hyperledger Projects - Hyperledger Consortiums and Networks - Hyperledger and Blockchain as a Service (BaaS).Case Study: Retail Banking

DECENTRALIZED APPLICATION **L: 9**

Solidity Language - Layout of a Solidity Source File - Structure of a contract - Functions - Scoping and declarations - Creating contracts - high level language features - Visibility and Getters - Decentralized Applications architecture - Connecting to the Blockchain and Smart Contracts – Building dApps – Deployment.

REFERENCES:

1. Ramchandra Sharad Mangrulkar and Pallavi Vijay Chavan, (2024), Blockchain Essentials Core Concepts and Implementations, Apress publications.
2. Drescher, D. (2018). Blockchain basics: A non-technical introduction in 25 steps, Apress.
3. Bashir, I. (2018). Mastering blockchain: Unlocking the power of cryptocurrencies, smart contracts, and decentralized applications, Packt Publishing.
4. Gupta, M. (2018). Blockchain basics: A primer for principals. Independently published.

5. Mougayar, W. (2016). The business blockchain: Promise, practice, and application of the next internet technology, Wiley.
6. Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind Bitcoin and other cryptocurrencies is changing the world. Portfolio.

L: 45; TOTAL: 45 PERIODS

Course Code	IOT SECURITY	L	T	P	E	C
23IC08E		3	0	0	0	3

COURSE OUTCOMES

Upon the successful completion of the course, the student will be able to

Theory Component

CO1: Analyze the fundamentals of Internet of Things (IoT) architecture and protocols to identify potential security vulnerabilities and threats.
CO2: Design and implement cryptographic techniques and protocols for securing IoT devices, communications, and data.
CO3: Evaluate security mechanisms for IoT networks, including authentication, access control, and intrusion detection systems.
CO4: Assess the security risks associated with IoT applications, services, and ecosystems, and devise strategies for mitigating these risks.
CO5: Develop and deploy secure IoT solutions using best practices, standards, and frameworks.
CO6: Communicate effectively and collaborate with multidisciplinary teams to address complex IoT security challenges and present solutions.

CO1: Analyze the fundamentals of Internet of Things (IoT) architecture and protocols to identify potential security vulnerabilities and threats. **L:9**

Introduction to IoT architecture - Components of IoT systems - IoT communication protocols - Sensor networks and data acquisition - IoT Connectivity - Vulnerabilities in IoT devices and networks - Security Architecture for IoT-IoT Security Standards and Regulations - Secure software development lifecycle (SDLC) for IoT.

CO2: Design and implement cryptographic techniques and protocols for securing IoT devices, communications, and data. **L: 9**

Threat Modeling in IoT Security - Identifying potential threats to IoT systems - IoT Device Hardening Firmware security updates and patch management - Authentication protocols for IoT devices Access Control in IoT Environments - Role-based access control (RBAC) for IoT applications Access control enforcement mechanisms - Transport Layer Security (TLS) in IoT communications Securing MQTT, CoAP, and other IoT protocols - IoT Security Monitoring and Incident Response Real-time monitoring of IoT device behavior.

CO3: Evaluate security mechanisms for IoT networks, including authentication, access control, and intrusion detection systems. **L:9**

Secure Bootstrapping - Secure key establishment mechanisms - Bootstrapping protocols (e.g., DTLS, SCEP) - Remote device management and monitoring - Techniques for secure data transmission - Message integrity and authenticity verification - Blockchain for IoT Security - Integration of blockchain with IoT systems - Decentralized identity and access management - Post-Quantum Cryptography - Hardware Security for IoT Devices - Hardware-based security mechanisms (e.g., Trusted Execution Environment)- Machine Learning for IoT Security.

CO4: Assess the security risks associated with IoT applications, services, and ecosystems, and devise strategies for mitigating these risks. **L: 9**

Zero Trust Security for IoT - Zero trust architecture principles -Micro-segmentation and network isolation in IoT - Firmware Security - Supply Chain Security- Vendor risk management and third-party assessments - Proactive threat hunting techniques - Principles of secure coding in embedded systems- Code review and static analysis tools -IoT Security Policies and Compliance.

CO5: Develop and deploy secure IoT solutions using best practices, standards, and frameworks. **L: 9**

Incident Response and Disaster Recovery Planning - Developing incident response plans for IoT security breaches - Disaster recovery strategies for IoT systems- Testing and exercising incident response plans - Real-time threat detection and response mechanisms - Security information and event management (SIEM) - Roles and responsibilities in IoT security management - Board-level oversight and accountability for IoT security - Incorporating security by design principles into IoT product development - Threat modeling techniques for IoT systems- Industry standards for IoT security (e.g., ISO/IEC 27001, NIST).

REFERENCES:

1. Shancang Li, Li Da Xu, and Shanshan Zhao, "Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations", Wiley, 2016.
2. Rolf Oppliger, "Security Technologies for the World Wide Web", Artech House, 2002.
3. Nils Gruschka, Christian Krauß, "Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications", Wiley, 2017.
4. Christopher Kruegel, William Robertson, and Giovanni Vigna, "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws", Wiley, 2011.
5. David Etter, "Principles of Information Security", Cengage Learning, 2016.

L: 45; TOTAL: 45 PERIODS

23IC09E **ANDROID SECURITY** **L T P C**
3 0 0 3

COURSE OUTCOMES

Upon completing of this course, the students will be able to

CO1: Explore the basics of Android Security Architecture
CO2: Elaborate the concepts of application frameworks.
CO3: Analyze the requirement for android security in wireless and mobile network.
CO4: Apply the concepts of cryptography for Android device security.
CO5: Apply the various testing techniques in Android application.

INTRODUCTION TO ANDROID'S SECURITY MODEL AND PERMISSIONS **8**

Android's Architecture – Android's Security Model –Permissions - Permission Enforcement - System Permissions - Custom Permissions - Activity and Service Permissions - Broadcast Permissions - Content Provider Permissions.

ANDROID'S PACKAGE AND USER MANAGEMENT **9**

Android Application Package Format - Code Signing- APK Install Process -Package Verification - Multi-User Support Overview - Types of Users - User Management - User Metadata - Per-User Application Management - External Storage.

ANDROID'S NETWORK SECURITY, PKI, AND CREDENTIAL STORAGE **10**

PKI and SSL Overview- JSSE Introduction- Android JSSE Implementation- VPN and Wi-Fi EAP Credentials- Credential Storage Implementation- Public APIs- Account Management Implementation - Google Accounts Support.

ANDROID'S ENTERPRISE AND DEVICE SECURITY **9**

Device Administration - VPN Support - Wi-Fi EAP - Controlling OS Boot-Up and Installation - Verified Boot - Disk Encryption - Screen Security - Secure USB Debugging - Android Backup - NFC Overview - Android NFC Support - Secure Elements - Software Card Emulation.

ANDROID APP TESTING TECHNIQUES **9**

Static analysis - Dynamic analysis - Penetration testing – Authentication and Authorization testing- Integrity testing – Data storage testing - User Input Validation Testing - Security Compliance Testing.

L: 45; TOTAL: 45 PERIODS

REFERENCES

1. Gerardus Blokdyk, "Android Security - A Complete Guide", 2020 Edition, 5STARCooks, 2020.
2. William Confer and William Robert, "Android Security: Attacks and Defenses" Packt publishing, 2015.
3. Nikolay Elenkov, "Android Security Internals: An In-Depth Guide to Android's Security Architecture" - No Starch Press publishing, US; Combined edition, 2014.
4. Keith Makan, Scott Alexander-Bown, Keith Harald Esrick Makan, "Android Security Cookbook" – Packt publishing, 2013.

Course Code	SECURITY IN SOFTWARE DEFINED NETWORKING	L	T	P	E	C
23IC10E		3	0	0	0	3

COURSE OUTCOMES

Upon the successful completion of the course, the student will be able to

Theory Component

CO1: identify the components and functions of virtual networking environments.
CO2: describe the fundamental principles, architecture and methodologies of SDN/NFV.
CO3: analyze potential attack vectors and security risks associated with SDN controllers, data planes, and VNFs.
CO4: explore the mechanisms and strategies used in microsegmentation and Moving target defense to dynamically change system configurations.
CO5: analyze potential attack vectors and their impact on distributed SDN infrastructures.

FUNDAMENTALS OF VIRTUAL NETWORKING AND SECURITY **L:9**

Foundations of computer networks – Address: MAC, IPV4, IPV6, Port – Physical, logical and overlay networks – Services – Routing – Virtual Networking: Introduction – Layer 2 Virtual Networking – Tunneling protocols and Virtual Private Networks – Virtual Routing and Forwarding.

SDN AND NFV **L: 9**

Introduction – Network functions virtualization – Software Defined Networking – Routing in SDN – P4 Programming model – P4 programming language – Protocol independent switch architecture – Network Security: Basics of Computer Network Security – network Reconnaissance – Preventive techniques – Detection and Monitoring – Network security Assessment.

SDN AND NFV SECURITY **L:9**

Introduction – Security challenges in NFV – NFV Security – NFV Security Lifecycle – NFV Security Countermeasures – SDN Security: SDN Security classification – Design of secure and dependable SDN platform – SDN data plane attacks – SDN specific security challenges – Open flow protocol and open flow switch security analysis.

SECURITY METHODS **L: 9**

Distributed Firewalls - Microsegmentation: Introduction – Design considerations – Microsegmentation defined – NIST cyber security recommendations – Case study: VMware NSX microsegmentation.

Moving Target Defense (MTD): Introduction – Classification – SDN based MTD – Game Theoretic MTD models – Evaluation of MTD.

SECURITY IN DISTRIBUTED SDN **L: 9**

Service Function Chaining (SFC): Introduction – SDN and NFV based SFC – SFC Implementation – Policy aware SFC – Secure SFC – Security policy management: Flow rules – Flow rule management challenges – Flow rule conflicts – Controller Decentralization considerations – Flow rule conflict resolution – Resolution model – Intelligent Software defined security.

REFERENCES:

1. Dijiang Huang, Ankur Chowdhary, Sandeep Pisharody, “Software-Defined Networking and Security from Theory to Practice”, First Edition, CRC Press, 2019.
2. Michael Goodrich Irvine Roberto Tamassia, “Introduction to Computer Security”, First Edition, Pearson new international edition, 2022.
3. Guy Pujolle , “Software Networks : Virtualization, SDN, 5G, and Security” , Second Edition, Wiley Publisher, 2020.
4. S. Scott-Hayward, S. Natarajan and S. Sezer, "A Survey of Security in Software Defined Networks," in IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 623-654.
5. Paul Goransson and Chuck Black, “Software Defined Networks: A Comprehensive Approach”, Second Edition, Morgan Kaufmann publishers, 2016.

L: 45; TOTAL: 45 PERIODS

Course Code	BIOMETRIC SECURITY ANALYSIS	L	T	P	E	C
23IC11E		3	0	0	0	3

COURSE OUTCOMES

Upon the successful completion of the course, the student will be able to

Theory Component

CO1: describe the basic physical and biological science and engineering principles.
CO2: analyze and design the biometric system applications at the component level.
CO3: work effectively in teams and express their work and ideas orally and in writing.
CO4: Identify the sociological and acceptance issues in biometric systems.
CO5: analyze various Biometric security issues.

CO1: describe the basic physical and biological science and engineering principles. **L:9**

Biometrics- Introduction- benefits of biometrics over traditional authentication systems - benefits of biometrics in identification systems-selecting a biometric for a system –

Applications – Key biometric terms and processes - biometric matching methods –Accuracy in biometric systems.

CO2: analyze and design the biometric system applications at the component level. **L: 9**

Physiological Biometric Technologies: Fingerprints – Technical description –characteristics - Competing technologies - strengths – weaknesses – deployment - Facial scan - Technical description - characteristics - weaknesses-deployment - Iris scan – Technical description – characteristics - strengths – weaknesses – deployment - Retina vascular pattern

CO3: work effectively in teams and express their work and ideas orally and in writing. **L:9**

Technical description – characteristics - strengths – weaknesses – deployment - Hand scan - Technical description-characteristics - strengths – weaknesses deployment – DNA biometrics.

Behavioral Biometric Technologies: Handprint Biometrics – DNA Biometrics.

CO4: Identify the sociological and acceptance issues in biometric systems **L: 9**

Signature and handwriting technology - Technical description – classification – keyboard / keystroke dynamics- Voice – data acquisition - feature extraction - characteristics - strengths – Weaknesses-deployment.

CO5: analyze various Biometric security issues. **L: 9**

Multi biometrics and multi factor biometrics - two-factor authentication with passwords - tickets and tokens – executive decision - implementation plan.

REFERENCES:

1. Jiankun Hu, David Chek Ling Ngo, Andrew Beng Jin Teoh,"Biometric Security", Cambridge Scholars Publishing, 2015.
2. Samir Nanavathi, Michel Thieme, and Raj Nanavathi, "Biometrics -Identity verification in a network", 1st Edition, Wiley Eastern, 2002.
3. John Berger: "Biometrics for Network Security", 1st Edition, Prentice Hall, 2004.
4. John Chirillo and Scott Blaul, "Implementing Biometric Security", 1st Edition, Wiley Eastern Publication, 2005.

L: 45; TOTAL: 45 PERIODS

23IC12E **MALWARE ANALYSIS** **L T P C**
3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: Learn to analyze the various malwares and malware analysis.
CO2: Perform basic static analysis with various tools
CO3: Analyze the malware behavior in windows
CO4: Perform basic dynamic analysis with tools
CO5: Apply malware classification and functionality.

INTRODUCTION TO MALWARE ANALYS **9**

Types of Malwares - Historical perspective on malware - The goal of malware analysis - Types of malware analysis - Introduction to virtualization and its role in malware analysis – Configuration - Setting up a safe environment for malware analysis.

ADVANCED STATIC ANALYSIS **8**

Levels of Abstraction - Reverse-Engineering - The x86 Architecture - Loading an Executable - The IDA Pro Interface - Cross-References - Analyzing Functions - Graphing Options - Enhancing Disassembly - Extending IDA with Plug-ins.

ANALYZING MALICIOUS WINDOWS PROGRAMS **10**

Classification of malicious Windows programs - File format analysis (PE files, DLLs)- Strings and binary analysis - Windows API - Windows Registry - Networking APIs - WinINet API - Running Malware – Kernel vs User mode - The Native API.

ADVANCED DYNAMIC ANALYSIS **9**

DEBUGGING: Source-Level vs. Assembly-Level Debuggers - Kernel vs. User-Mode Debugging - Exceptions - Modifying Execution with a Debugger - OLLYDBG: Loading Malware - The OllyDbg Interface - Memory Map - Threads and Stacks - Executing Code – Breakpoints - Loading DLLs – Tracing.

MALWARE FUNCTIONALITY **9**

MALWARE BEHAVIOR Downloaders and Launchers - Backdoors - Credential Stealers - Privilege Escalation - User-Mode Rootkits – Launchers - Process Injection - Process Replacement – Hook Injection – APC Injection - Network Countermeasures - Safely Investigate an Attacker Online - Content-Based Network Countermeasures.

L: 45; TOTAL: 45 PERIODS

REFERENCES

1. NirYehoshua, Uriel Kosayev, “Antivirus Bypass Techniques: Learn practical techniques and tactics to combat, bypass, and evade antivirus software”, 1st Edition, Packt Publishing, 2021.
2. Alexey Kleymenov, Amr Thabet, “Mastering Malware Analysis: The complete malware analyst's guide to combating malicious software, APT, cybercrime, and IoT attacks”, 1st Edition, Packt Publishing, 2019.
3. Pavel Yosifovitch, “Windows Kernel Programming”, 1st Edition, Packt Publishing, 2019.
4. Michael Sikorski and Andrew Honig, “Practical Malware Analysis, The Hands-On Guide to Dissecting Malicious Software”. No Starch Press, 2012.

23IC13E **WEB APPLICATION SECURITY** **L T P C**
3 0 0 3

COURSE OUTCOMES

Upon completing the course, the students will be able to:

CO1: elaborate on the significance of web application and its security.
CO2: apply suitable authentication mechanism to solve a problem web application.
CO3: analyze the various security threats for maintaining secure database and counter measures.
CO4: interpret the security testing tools and methodologies to identify and address potential vulnerabilities within web applications.

WEB APPLICATION SECURITY FUNDAMENTALS **9**

Introduction of Web Application security- OWASP-Input Validation-Attack Surface Reduction-Classifying and Prioritizing Threats

WEB APPLICATION-AUTHENTICATION PRINCIPLES **9**

Access Control Overview-Authentication Fundamentals-Web Application Authentication-Securing Password based Authentication-Authorization Session Management Fundamentals-Securing Web Application Session Management

BROWSER SECURITY PRINCIPLES **9**

Same-Origin Policy-HTML Element-JSON and JSONP-XMLHttpRequest - iframes and JavaScript document domain-Cross-Site Scripting-Cross-Site Request Forgery

DATABASE SECURITY **9**

SQL Injection-Setting Database Permissions-Stored Procedure Security-File Security-Forceful Browsing-Directory traversal

SECURE DEVELOPMENT AND DEPLOYMENT **9**

Security Testing-Security Incident Response Planning-Secure development methodologies-Microsoft Security Development Lifecycle (MSDL) - OWASP Comprehensive Lightweight Application Security Process (CLASP)

L: 45; TOTAL: 45 PERIODS

REFERENCES

1. Andrew Hoffman, “Web Application Security: Exploitation and Countermeasures for Modern Web Applications, O’Reilly Media, Inc,, 1st Edition, 2020.
2. Ravi Das and Greg Johnson, “Testing and Securing Web Applications”, Taylor & Francis Group, LLC, 2021.
3. Prabath Siriwardena, “Advanced API Security”, Apress Media LLC, USA, 2020.
4. Malcom McDonald, “Web Security for Developers”, 2020, No Starch Press, Inc.
5. Neil Madden, “API Security in Action”, 2020, Manning Publications Co., NY, USA.
6. Bryan Sullivan, Vincent Liu, “Web Application Security: A Beginners Guide”, 2012, The McGraw-Hill Companies.
7. Michael Cross, “Developer’s Guide to Web Application Security”, 2007, Syngress Publishing, Inc.
8. Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, and Terron Williams Grey Hat,” Hacking: The Ethical Hacker’s Handbook”, 3rd Edition, 2011, The McGraw-Hill Companies.

23IC14E **MULTIMEDIA SECURITY** **L T P C**
3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: identify multiple issues related to the protection of digital media, including audio, image, and video content.
CO2: explore various encryption approaches for protecting multimedia contents such as image, video and audio.
CO3: illustrates image, video and audio authentication for multimedia authentication.
CO4:analyse robust watermarking techniques to enhance the resilience of multimedia fingerprints against various attacks.
CO5: inspect various protocols for achieving anonymous communication in multimedia networks.

INTRODUCTION **9**

Introduction to Multimedia System, Multimedia Files: Image and sound file formats, features of software to read and write such files, Basics of digital audio, Basics of digital imaging, Multimedia compression technologies and standards - VCD, DVD – MPEG1/2/4/21.

MULTIMEDIA ENCRYPTION **9**

Fundamentals of modern encryption - Multimedia encryption paradigm – Multimedia encryption schemes: Full Encryption, Selective Encryption, Joint Compression and Encryption, Syntax-Compliant Encryption, Scalable Encryption and Multi-Access Encryption – Image and video encryption schemes

MULTIMEDIA AUTHENTICATION **10**

Data Authentication – One way Hash functions – Message authentication code – Multimedia Authentication: Parameterization, Watermarking-Based Authentication – Image authentication – video Authentication – Audio Authentication.

MULTIMEDIA FINGERPRINTING **9**

Multimedia Fingerprinting: Steganography – Marking assumptions – Collusion attacks – Frame proof and anti-collusion codes – Coded finger printing modulation – semi fragile finger printing – Multicasting fingerprinting – Efficient security architectures: WHIM, Water casting, Chameleoncipher – Joint fingerprinting and decryption Framework – Finger casting.

PRIVACY PRESERVATION PROTOCOLS **8**

Zero knowledge protocols – Anonymous fingerprinting – Public Key watermarking.
Multimedia Security Applications: Media Sensor Network - Voice over IP (VoIP) Security – DTH – Video Conference

L: 45, TOTAL: 45 PERIODS

REFERENCES

1 William Puech, “Multimedia Security, Volume 1: Authentication and Data Hiding”, First Edition, Wiley-ISTE, 2022.
2 Frank Y. Shih, “Multimedia Security: Watermarking, Steganography, and Forensics”, First Edition, CRC Press, 2013.
3 Chun-Shien Lu, “Multimedia Security: Steganography and Digital Watermarking techniques for Protection of Intellectual Property”, First Edition, Springer US, 2007.
4 Wenjun Zeng, Heather Yu, Ching-Yung Lin, “Multimedia Security Technologies for Digital Rights Management”, First Edition, Elsevier (AP), 2006.
5 Borko Furht, Darko Kirovski, “Multimedia security handbook”, First Edition, CRC Press, 2005.

Course Code	ENTERPRISE CYBER SECURITY	L	T	P	E	C
23IC15E		3	0	0	0	3

COURSE OUTCOMES

Upon the successful completion of the course, the student will be able to

Theory Component

CO1: discriminate and analyze problems involved in cybercrime
CO2: synthesis cybercrime issues on wireless and mobile devices
CO3: identify the methods used for a cyber crime attack
CO4: analyze the computer forensic problems for a feasible solution
CO5: apply cyber law for a given type of cyber issues

INTRODUCTION TO CYBERCRIME **L:9**

Overview to Cybercrime- Cybercrime and Information Security-Classifications of Cybercrimes- Cybercrime: The Legal Perspectives, Cybercrimes: Perspective, Cybercrime and the Indian ITA 2000- A Global Perspective on Cybercrimes -Cyber offenses: How Criminals Plan Them: How Criminals Plan the Attacks, Social Cyber stalking Cyber cafe and Cybercrimes.

CYBERCRIME: MOBILE AND WIRELESS DEVICES **L: 9**

Cybercrime: Mobile and Wireless Devices-Proliferation of Mobile and Wireless Devices-Credit Card Frauds in Mobile and Wireless Computing Era- Security Challenges Posed by Mobile Devices and Registry Settings for Mobile Devices-Attacks on Mobile/Cell Phones-Organizational Security Policies and Measures in Mobile Computing.

METHODS USED IN CYBERCRIME **L:9**

Methods Used in Cybercrime: Proxy Servers and Anonymizers-Phishing-Password Cracking- Key loggers and Spywares- Virus and Worms- Trojan Horses and Backdoors-Steganography- DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks.

COMPUTER FORENSICS **L: 9**

Overview of Computer Forensics-Digital Forensics Science-The Need for Computer Cyber forensics and Digital Evidence-Forensics Analysis of EMail- Digital Forensics Life Cycle-Chain of Custody Concept- Network Forensics- Approaching a Computer Forensics Investigation- Forensics and Social Networking Sites: The Security/Privacy Threats-Computer Forensics from Compliance Perspective- Challenges in Computer Forensics-Special Tools and Techniques- Forensics Auditing- Anti forensics.

CYBERCRIMES AND CYBER SECURITY **L: 9**

The Legal Perspectives on Cybercrimes and Cyber security: The legal landscape around the world- Need of Cyber laws in the Indian context- The Indian IT Act-Digital signatures and The Indian IT Act- Amendments to The Indian IT Act-Cybercrime and Punishment.

REFERENCES:

1. Jeff Kosseff, “Cyber Security Law”, John Wiley & Sons, 2020.
2. Dr. Surya Prakash Tripathi, Ritendra Goyal, Praveen Kumar Shukla, KLSI. “Introduction to information security and cyber laws”. Dreamtech Pre ss. ISBN: 9789351194736, 2015.
3. Thomas J. Mowbray, “Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions”, Copyright © 2014 by John Wiley & Sons, Inc, ISBN: 91-118 -

84965 -1.

4. Sunit Belapure and Nina Godbole, “Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives”, Wiley India Pvt Ltd, ISBN: 978-81-265-21791, Publish Date 2013.
5. James Graham, Ryan Olson, Rick Howard, “Cyber Security Essentials”, CRC Press, 15-Dec-2010.

L: 45; TOTAL: 45 PERIODS

Course Code	DISTRIBUTED SYSTEM SECURITY	L	T	P	E	C
23IC16E		3	0	0	0	3

COURSE OUTCOMES

Upon the successful completion of the course, the student will be able to

Theory Component

CO1: Identify the concepts of Common Security Issues and Security Techniques.
CO2: Summarize the importance of security engineering ideas, threads and Vulnerability
CO3: Evaluate the concepts of Security Solution related to distributed systems security.
CO4: Analyze the importance of Multi Lateral Security in Distributed Systems.
CO5: Explore the emerging security challenges in distributed System security.

OVERVIEW OF DISTRIBUTED SYSTEM SECURITY **L:9**

Common Security Issues- Common Security Techniques-Privacy –Identity Management-Digital Signatures-Message Authentication Codes-Authentication Mechanisms-Public Key Infrastructure-Models of Trust-Authorization-Firewalls-Security Policies and Enforcement Mechanisms.

SECURITY ENGINEERING **L: 9**

Secure Development Lifecycle Processes Overview- Security Engineering Process-Important Security Engineering Guidelines and Resources- Host-level threats and vulnerabilities - Infrastructure-level threats and vulnerabilities – Application level threats and vulnerabilities - Service-level threats and vulnerabilities.

SECURITY SOLUTION **L:9**

Host-level solutions - Infrastructure-level solutions - Application-level solutions - Service-level solutions. Container Security –SOA Security Standard Stack-Web Services Security-Security Assertions Markup Language-Deployment architectures for SOA Security - Managing Service Level Threads-Network Level Solutions.

MULTILATERAL SECURITY **L: 9**

Compartmentation and the Lattice Model- The Chinese Wall- The BMA Model- The Threat Model- Current Privacy Issues– Inference Control- Randomization- Active Attacks- The Value of Imperfect Protection - The Residual Problem.

EMERGING TRENDS **L: 9**

Security challenges in edge computing - fog computing- SOX Compliance - SOX Security Solutions - Multilevel Policy-Driven Solution Architecture - The Financial Application - Security Requirements Analysis - Final Security Architecture.

REFERENCES:

1. Abhijit Belapurkar, Anirban Chakrabarti, Harigopal Ponnapalli, Niranjan Varadarajan, Srinivas Padmanabhuni, Srikanth Sundarrajan, “Distributed Systems Security: Issues, Processes and Solution” Third Edition, John Wiley & Sons Ltd, 2018.
2. Ross J. Anderson "Security Engineering: A Guide to Building Dependable Distributed Systems” second edition Tata McGraw-Hill Publishing Company Limited, New Delhi 2020.

L: 45; TOTAL: 45 PERIODS

Course Code	E – COMMERCE SECURITY	L	T	P	E	C
23IC17E		3	0	0	0	3

COURSE OUTCOMES

Upon the successful completion of the course, the student will be able to

Theory Component

CO1: Explain the basic concepts, theories, and business models underlying e- commerce.
CO2: Analyze the importance of security and trust in e-commerce, and be able to realize techniques to foster the process of doing business on the Web.
CO3: Explain the added value, risks and barriers in the adoption of e-Business and E-Commerce.
CO4:Comprehend the important issues in design and development, such as website effectiveness, usability, brand strategy, and personalizing the user experience.
CO5: Apply necessary tools and information to design and build systems that take advantage of trusted computing

INTRODUCTION TO E-COMMERCE **L:9**

Network and E-Commerce – Types of E-Commerce – E-Commerce Business Models: B2C, B2B, C2C, P2P and M-commerce business models – Ecommerce.

PAYMENT SYSTEMS & SECURITY **L: 9**

Types of payment system – Credit card E-Commerce transactions– B2C E-Commerce Digital payment systems – B2B payment system.E-Commerce Security Environment – Security threats in E-Commerce environment – Policies, Procedures and Laws

INTER-ORGANIZATIONAL TRUST IN E-COMMERCE **L:9**

Need – Trading partner trust – Perceived benefits and risks of E-Commerce – Technology trust mechanism in E-Commerce – Perspectives of organizational, economic and political theories of inter-organizational trust – Conceptual model of inter-organizational trust in E-Commerce participation.

INTRODUCTION TO TRUSTED COMPUTING PLATFORM **L: 9**

Overview – Usage Scenarios – Key components of trusted platform – Trust mechanisms in a trusted platform.

PLATFORMS & MODELS **L: 9**

Secured platforms for organizations and individuals – Trust models and the E-Commerce domain.

REFERENCES:

1. Gulshan Yadav, “E-Commerce Security: An Introduction to Secure E-Commerce”, 2017.

2. Gary Schneider, “Electronic Commerce”, Course Technologies, Sixth Edition, 2006.
3. Kenneth C. Laudon and Carol Guercio Trave, “E-Commerce Business Technology Society”, Pearson Education, 2005.
4. Pauline Ratnasingam, “Inter-Organizational Trust for Business-to-Business E- Commerce” IRM Press, 2005.
5. Siani Pearson, et al, “Trusted Computing Platforms: TCPA Technology in Context”, Prentice Hall PTR, 2002.

L: 45; TOTAL: 45 PERIODS

Course Code	OPERATING SYSTEMS SECURITY	L	T	P	E	C
23IC18E		3	0	0	0	3

COURSE OUTCOMES

Upon the successful completion of the course, the student will be able to

Theory Component

CO1: Relate the concepts of a security environment and the principles of controlling access to system resources.

CO2: Evaluate and select appropriate tools for specific security tasks.

CO3: Analyze and design protection systems to safeguard resources and ensure secure access control.

CO4: Analyze various models to enforce information flow secrecy and integrity.

CO5: Apply strategies to address the security challenges and enhance the overall security posture of systems.

OPERATING SYSTEM FUNDAMENTALS **L:9**

Fundamentals **–** OS Processes **–** Synchronization **–** Memory Management **–** File Systems **–** Security Environment – Controlling Access to the Resources – Formal models of Secure Systems – Cryptography – Authentication – Exploiting Software – Insider Attacks – Malware.

OS HARDENING AND PROTECTION METHODS **L: 9**

OS Hardening : System Hardening – Classic Hardening on Servers – Log Files and Unnecessary Services and Accounts – Configuring Accounts – Patching – System Auditing – OS Protection Methods – OS Firewalls – OS Security Tools – Trusted Operating Systems – Assurance in Trusted Operating Systems.

ACCESS CONTROL FUNDAMENTALS AND MULTICS **L:9**

Secure operating systems – Security goals – Trust model – Threat model – Access Control Fundamentals – Protection system – Lampson's Access Matrix – Reference monitor. Multics – Multics system – Multics security – Vulnerability analysis – Security in ordinary OS – Unix, Windows, Mac.

VERIFIABLE SECURITY GOALS **L: 9**

Verifiable security goals – Information flow – Information flow secrecy models: Denning's Lattice model – Bell-LaPadula model – Information flow integrity models: Biba integrity model – Low water Mark Integrity – Clark-Wilson integrity – Challenges of Trusted Processes – Covert channels.

SECURITY KERNELS **L: 9**

Security Kernels – Secure Communications processor – Securing Commercial OS – Secure Capability Systems – Fundamentals – Security Challenges – Secure Virtual Machine Systems.

REFERENCES:

1. Andrew S Tanenbaum and Herbert Bos, "Modern Operating Systems", 5th Edition, Pearson, 2023.
2. Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, "Security in Computing", 5th Edition, Prentice Hall, 2015.
3. Enrico Perla and Massimiliano Oldani, "A Guide to Kernel Exploitation Attacking the Core", Elsevier, 2011.
4. Trent Jaeger, Operating System Security, Synthesis Lectures on Information Security, Privacy and Trust, Springer, 2008.

L: 45; TOTAL: 45 PERIODS

23IC19E **SOCIAL NETWORK SECURITY LABORATORY** **L T P C**
0 0 4 2

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: demonstrate password management, email attack and authentication using LastPass.

CO2: demonstrate access restrictions, firewall, and network security in social media using Hotspot Shield VPN

LIST OF EXERCISES

1. Simulation of Phishing email attack using LastPass
2. Simulation of Impersonation attack on social network
3. Implementation of password generation and strengthen improvement in social network
4. Simulation of Two Factor authentication usage in Social network.
5. Simulate Hotspot Shield VPN can enable access to geographically restricted social network content.
6. Simulate public Wi-Fi networks Hotspot Shield VPN when accessing social networks and personal accounts.
7. Implementation of bypassing network restrictions, simulate online security while travel using Hotspot Shield VPN.
8. Simulate various strategies for secure browsing in social media sites.

P: 30; TOTAL: 30 PERIODS

23IC20E **ANDROID SECURITY LABORATORY** **L T P C**
0 0 4 2

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: Identify and analyze common security vulnerabilities in Android applications.

CO2: Demonstrate the ability to assess the security of third-party apps.

LIST OF EXERCISES

1. Install and set up Android Studio with the latest security patches.
2. Create a simple Android app with various permissions.
3. Create a vulnerable Android app with intentional security flaws.
4. Select a target Android app for penetration testing.
5. Obtain Android malware samples for analysis.
6. Assess its security implications and integrate it into a sample app securely.
7. Debug a simple Android app to understand its runtime behavior and use reverse engineering tools to analyze the app's structure.

P: 30; TOTAL: 30 PERIODS

Course Code	PRINCIPLES OF DIGITAL FORENSICS	L	T	P	E	C
23IC21E		3	0	0	0	3

COURSE OUTCOMES

Upon the successful completion of the course, the student will be able to

Theory Component

CO1: explore the knowledge of digital forensics in both business and private world.
CO2: apply authentication methods to ensure the integrity and reliability of acquired digital evidence.
CO3: recognize current techniques and tools for forensic investigations.
CO4: evaluate and perform forensic analysis in various fields.
CO5: analyze the procedures for network and mobile device forensics.

INTRODUCTION TO DIGITAL FORENSICS **L:9**

Overview of Digital Forensics – Rules for Digital Forensic, Need for Digital Forensics, Types of Digital Forensics, Ethics in Digital Forensics, Introduction to Internet Crimes, Hacking and Cracking, Credit Card and ATM Frauds, Web Technology, Cryptography.

DIGITAL FORENSIC ACQUISITION AND AUTHENTICATION **L: 9**

Storage formats for digital evidence – Image acquisition – acquisition tools – authenticating data acquisition – RAID data acquisition – Remote Network acquisition tools.

DIGITAL FORENSICS TOOLS **L:9**

Software Tools: Command-Line – Linux - Other GUI – Hardware Tools: Workstations - Write-Blocker - Validating and Testing Forensics Software - Case Studies: Digital Evidence Acquisition using FTK and Nmap Tools.

DIGITAL FORENSIC ANALYSIS AND VALIDATION **L: 9**

Principles of Digital Forensic Data collection and Analysis - Validating Forensic Data - Addressing Data-Hiding Techniques – Case Studies.

NETWORK AND MOBILE DEVICE FORENSICS **L: 9**

Network Forensics: Securing a Network- Procedures for Network Forensics - Examining the Honeynet Project - Mobile Device Forensics: Understanding Mobile Device Forensics - Acquisition Procedures for Mobile Devices.

REFERENCES:

1. Joakim Kävrestad, Marcus Birath, Nathan Clarke, “Fundamentals of Digital Forensics: A Guide to Theory, Theory and Applications, Springer, Third Edition, 2024.
2. Shiva V. N. Parasram, ”Digital Forensics with Kali Linux , Packet Publishing Pvt Ltd ,Third Edition, 2023.
3. Deepak Rawtani, Chaudhery Mustansar Hussain, “Modern Forensic Tools and Devices: Trends in Criminal Investigation”, Scrivener Publishing, 2023.
4. Bill Nelson, Amelia Phillips, Christopher Steuart, “Guide to Computer Forensics and Investigations”, Cengage Learning, Sixth Edition, 2020.
5. Gerard Johansen, “Digital Forensics Incident Response tools and techniques for effective cyber threat response” Packet Publishing, 2022.

L: 45; TOTAL: 45 PERIODS

23IC22E PENETRATION TESTING AND VULNERABILITY ASSESSMENT

L	T	P	C
3	0	0	3

Prerequisites:

1. Knowledge in information security.
2. Knowledge in web application

COURSE OUTCOMES

CO1: Analyze and evaluate social engineering attacks.
CO2: Discover how to handle vulnerabilities of Web Application.
CO3: Perform penetration testing.
CO4: Analyze the malware type and impact.
CO5: Analyze the outcome from the tools and technologies used by security analyst.
CO6: Analyze the vulnerability assessments in the form of penetration testing.

INTRODUCTION TO PENETRATION TESTING METHODOLOGIES **9**

Penetration Testing, Common Penetration Testing Techniques - Penetration Testing Process - Announced Testing/Unannounced Testing - Types of Penetration Testing - Strategies of Penetration Testing - Operational Strategies for Security Testing - Identifying Benefits of Each Test Type - Prioritizing the Systems for Testing - Phases of Penetration Testing.

PHYSICAL PENETRATION ATTACKS **9**

Defending against physical penetrations - Insider Attacks–Metasploit.

MANAGING A PENETRATION TEST **9**

Planning – structuring – Execution - information sharing reporting the results. Basic Linux Exploits: Stack Operations - Buffer Overflows - Local Buffer Overflow Exploits - Exploit Development Process. Windows Exploits: Compiling and Debugging Windows Programs - Writing Windows Exploits - Structured Exception Handling (SEH) - Windows Memory Protections (XPSP3, Vista, 7 and Server 2008) - Bypassing Windows Memory Protections.

WEB APPLICATION SECURITY VULNERABILITIES **9**

Overview of top web application security vulnerabilities - Injection vulnerabilities - cross-Site scripting vulnerabilities - OWASP Top Ten SQL Injection vulnerabilities - Cross-site scripting vulnerabilities. Vulnerability Analysis: Passive Analysis - Source Code Analysis - Binary Analysis.

CLIENT-SIDE BROWSER EXPLOITS **9**

History of client- side exploits and latest trends - finding new browser-based vulnerabilities heap spray to exploit - protecting 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.

L: 45; TOTAL: 45 PERIODS

REFERNCES

1. Allen Harper, Stephen Sims, Michael Baucom, "Gray Hat Hacking - The Ethical Hackers Hand book", Third Edition, Tata Mc Graw-Hill, 2018.
2. Dafydd Suttard, Marcus pinto, "Penetration Testing: Hands-on Introduction to Hacking", First Edition, Georgia Weidman, No Starch Press, 2007.
3. Phillip L. Wylie, Kim Crawley, "The Pen Tester Blueprint-Starting a Career as an Ethical Hacker ", First Edition, Wiley Publications, 2020.

Course Code	CYBER WARFARE IN INTELLIGENCE AND	L	T	P	E	C
23IC23E	MILITARY OPERATIONS	3	0	0	0	3

COURSE OUTCOMES

Upon the successful completion of the course, the student will be able to

Theory Component

CO1: compare the complexities of cyberspace conflicts in both theoretical and practical dimensions.

CO2: apply the international military doctrines for advanced analysis and military planning and operations.

CO3: identify intelligence operations into overall military and strategic planning to support and improve mission objectives.

CO4: apply defensive tactics and procedures in cyberspace attacks assess how existing military and intelligence planning considerations apply in cyberspace.

CYBER WARFARE **L:9**

Overview of Cyber Warfare-Tactical and operational reasons for Cyber War- Cyber Strategy and power- Cyber Arm controls- boundaries in Cyber Warfare-Cyber warfare Game theory- Game Theory in International Relations.

CYBER DOCTRINE **L: 9**

International Doctrine- Strategy from Around the World-Chinese Doctrine, European Countries- International preparation of the Operational Environment- Measures of Effectiveness- Battle Damage Assessment.

CYBER WARFARE IN INTELLIGENCE **L:9**

Tools and Techniques-Logical Weapons-Physical Weapons-Offensive Tactics and Procedures- intelligence and Counter Intelligence- Reconnaissance- Computer Networks attacks- Psychological Weapons.

DEFENSIVE TACTICS AND PROCEDURES **L: 9**

CIA Traid-Authenticate, Authorize and Audit (AAA)-Security Awareness and training-Surveillance, Data Mining and Patterns Matching- Vulnerabilities Assessment and

Penetration Testing- Defending against Cyber Attacks.

CYBERWARFARE AND INTERNATIONAL LAW **L: 9**

Principles of Just War - Law of Neutrality and Humanitarian Law - Ambiguity and Attribution - International Treaties - Characteristics of Confidence Building Measures.

References:

1. Peter Kestner,"The Art of Cyber Warfare: Strategic and Tactical Approaches for Attack and Defense in the Digital Age",2024, Springer.
2. Paul Rosenzweig, "Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World," Praeger, 2019.
3. Lech J. Janczewski, Lech J. Janczewski, Andrew M. Colarik, "Cyber warfare and cyber terrorism," First Edition, Information Science Reference, 2019.
4. Jason Andress and Steve Winterfeld, "Cyber Warfare, Techniques, Tactics, and Tools for Security Practioners", [2 ed.], Syngress, 2014.
5. Steve Winterfeld and Jason Andress, "The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice", 2012.

L: 45; TOTAL: 45 PERIODS

23IC24E CYBER SECURITY AND ETHICAL HACKING **L T P C**
3 0 0 3

COURSE OUTCOMES

CO1: choose the appropriate tools to support an ethical hack and defend the major issues.
CO2: interpret the results of a controlled attack in the area of cyber security
CO3: experience the role of politics, inherent and imposed limitations and metrics for planning of a test
CO4: comprehend the dangers associated with penetration testing

INTRODUCTION TO ETHICAL HACKING **9**

Hacking Impacts, The Hacker Framework: Planning the test, Sound Operations, Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Final Analysis, Deliverable, Integration. Information Security Models: Computer Security, Network Security, Service Security, Application Security, Security Architecture Information Security Program: The Process of Information Security, Component Parts of Information Security Program, Risk Analysis and Ethical Hacking.

THE BUSINESS PERSPECTIVE **9**

Business Objectives, Security Policy, Previous Test Results, Business Challenges. Planning for a Controlled Attack: Inherent Limitations, Imposed Limitations, timing is Everything, Attack Type, Source Point, Required Knowledge, Multi-Phased Attacks, Teaming and Attack Structure, Engagement Planner, The Right Security Consultant, The Tester, Logistics, Intermediates, Law Enforcement.

PREPARING FOR A HACK **9**

Technical Preparation, Managing the Engagement. Reconnaissance: Social Engineering, Physical Security, Internet Reconnaissance.

ENUMERATION **9**

Enumeration Techniques, Soft Objective, Looking Around or Attack, Elements of Enumeration, Preparing for the Next Phase. Exploitation: Intutive Testing, Evasion, Threads and Groups, Operating Systems, Password Crackers, RootKits, applications, Wardialing, Network, Service and Areas of Concern.

DELIVERABLE **9**

The Deliverable, The Document, Overal Structure, Aligning Findings, Presentation. Integration: Integrating the Results, Integration Summary, Mitigation, Defense Planning, Incident Management, Security Policy

L: 45; TOTAL: 45 PERIODS

REFERENCES

1. EC-Council, “Ethical Hacking and Countermeasures Attack Phases”, Cengage Learning, 2016.
2. James S. Tiller, “The Ethical Hack: A Framework for Business Value Penetration Testing”, Auerbach Publications, CRC Press, 2004.
3. Michael Simpson, Kent Backman, James Corley, “Hands-On Ethical Hacking and Network Defense”, Cengage Learning, 2010.

Course Code	FORENSICS AUDIO AND VIDEO ANALYSIS	L	T	P	E	C
23IC25E		3	0	0	0	3

COURSE OUTCOMES

Upon the successful completion of the course, the student will be able to

Theory Component

CO1: Understand the fundamentals of fuzzy logic operators and inference mechanisms
CO2: Understand neural network architecture for AI applications such as classification and clustering
CO3: Learn the functionality of Genetic Algorithms in Optimization problems
CO4: Use hybrid techniques involving Neural networks and Fuzzy logic
CO5: Apply soft computing techniques in solving problems and real-world applications

CO 1: Employ the fundamental knowledge of Audio Signals and Systems to forensic audio analyzing scenarios **L:9**

Fundamentals of Audio Signals and Systems -Wavelength, Frequency, and Spectrum, Human Hearing Characteristics, Signal Processing, Digital Audio, Perceptual Audio Coding. Introduction to Audio Forensics, Case studies - McKeever Case, The Watergate Tapes. asic Tools: Audio Playback, Waveform View and Spectrographic View - Audio Playback System, Waveform View, Spectrographic View.

CO 2. Demonstrate the current and emerging concepts and practices in the collection, processing, analyses, and evaluation of forensic evidence **L: 9**

Starting the Examination - Initial Aural Evaluation, Critical Listening, Waveform Analysis, Spectral Analysis. Authenticity Assessment - Authenticity of Analog Magnetic Tape Recordings and Authenticity of Digital Audio Recordings. Forensic Interpretation - Scientific Integrity, Methods and Reliability.

CO 3: comprehensive analysis of digital images from an entirely forensic standpoint **L:9**

Threats to the Integrity of Digital Media Content, Digital Content Protection, Digital Forensics- Image Source Identification, Image Forgery Detection. Camera Source Identification - Digital Camera Components, Source Camera Identification Framework - Motivation for Choice of Features, DCTR Feature Extraction, Feature Transformation by PCA, Classification, Ensemble Classifier. Copy-Move Forgery Detection in Digital Images - Overview of Existing Techniques, Classification of Block-Based Copy-Move Forgery Detection Techniques.

CO 4: analyze the appropriate computing requirements and interpret forensics data effectively **L: 9**

Collection of digital and analog audio and video, Physical examination of tapes for authenticity, Preparation of copies of recorded audio tapes, Preparation of enhanced copy of the recorded cassette, Transcription of the recorded cassette. Authentication, waveform analysis, magnetic development- Video Enhancement Techniques-Audio Enhancement Techniques- quality control and quality assurance performance.

CO5: analyze the given video frame and apply the appropriate techniques to distinguish the real video data from the unauthentic ally modified frame **L: 9**

DeepFake Detection - DeepFake Video Generation, Current DeepFake Detection Methods - General Principles, Categorization Based on Methodology, Categorization Based on Input Types, Categorization Based on Output Types, The DeepFake-o-Meter Platform, Datasets, Challenges. Video Frame Deletion Detection - Baseline Approaches, C3D Network for Frame Deletion Detection. Frame Duplication Detection - Coarse-Level Search for Duplicated Frame Sequences, Fine-Level Search for Duplicated Frames, Inconsistency Detector for Duplication Localization.

REFERENCES:

1. Robert C. Maher, “Principles of Forensic Audio Analysis”, Modern Acoustics and Signal Processing – Springer, 2018.
2. Husrev Taha Sencar, Luisa Verdoliva, Nasir Memon, “Multimedia Forensics”, Advances in Computer Vision and Pattern Recognition – Springer, 2022.
3. Aniket Roy, Rahul Dixit, Ruchira Naskar, Rajat Subhra Chakraborty, “Digital Image Forensics Theory and Implementation”, Studies in Computational Intelligence, Springer, 2020.
4. Stuart H. James, Jon J. Nordby , Suzanne Bell, Lana J Williams, “Forensic Science An Introduction to Scientific and Investigative Techniques”, CRC Press Taylor and Francis Group, 4th Edition, 2014.

L: 45; TOTAL: 45 PERIODS

Course Code	MOBILE DEVICE FORENSICS	L	T	P	E	C
23IC26E		3	0	0	0	3

COURSE OUTCOMES

Upon the successful completion of the course, the student will be able to

Theory Component

CO1: acquire proficiency in digital investigation techniques, including evidence handling and scene documentation.

CO2: acquire specialized expertise in iOS and Android forensics, focusing on data extraction methods and security mechanisms.
CO3: develop skills in analysing application artifacts on iOS and Android platforms.
CO4: evaluate forensic tools and techniques for both iOS and Android devices.
CO5: acquire competence in malware forensics, including analyzing volatile and non-volatile memory.

DIGITAL INVESTIGATION **L:9**

Evidence and Scene Security - Scene Documentation - Evidence Isolation - Prepare for Acquisition – Identification Phase – Collection Phase – Examination Phase.

ANDROID FORENSICS **L: 9**

Android File system – Android System Architecture – Android system Permission model – Harmony Operating System – Kernel Layer – Data Extraction Techniques on Android – Screen lock Bypassing Techniques - Mobile Forensics Investigation Challenges on Android Devices.

IOS FORENSICS **L:9**

iOS Boot Process - iOS Architecture - iOS Architecture Layers - The HFS Plus and PFS File Systems - iOS Security - iOS Data Extraction Techniques - Data Acquisition from Backup Devices - Data Acquisition from iOS Devices - Jailbreaking - iOS Forensic Tools - iOS Data Analysis and Recovery Using Belkasoft and Axiom Tool - Mobile Forensics Investigation Challenges on iOS Devices.

FORENSIC INVESTIGATIONS OF POPULAR APPLICATIONS ON ANDROID AND IOS PLATFORMS **L: 9**

Extracting Data of the Activities of the Instant Artifacts - Implementation and Examination Details - Results and Analysis - Acquisition for iOS - Acquisition for Android Device - Gmail Application Artifacts - iOS Seizure Device Information - Android OS - Forensic Tools Comparisons - Mobile Forensics for Google Drive - Cloud Storage Services Artifacts.

MALWARE FORENSICS FOR VOLATILE AND NONVOLATILE MEMORY IN MOBILE DEVICES **L: 9**

Mobile Malware Forensics - Smartphone Volatile Memory - Mobile Device Case Details and Experiment - Logical Acquisition - Physical Acquisition - iOS Analysis and Results - Evaluating Extraction Tools and Methods for Android and iOS Devices - Evaluating Android Extraction Techniques for Volatile and non-Volatile Memory.

REFERENCES:

1. Mohammed Moreb, “Practical Forensic Analysis of Artifacts on iOS and Android Devices Investigating Complex Mobile Devices” First Edition, 2022.
2. Lee Reiber, “Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation”, Second Edition, 2019.
3. Soufiane Tahiri, “Mastering Mobile Forensics”, 2016.
4. Heather Mahalik , Satish Bommisetty , and Rohit Tamma, “Practical Mobile Forensics" 1st Edition, 2014.

L: 45; TOTAL: 45 PERIODS

23IC27E CYBER SECURITY AND ETHICAL HACKING LABORATORY **L T P C**
0 0 4 2

COURSE OUTCOMES

CO1: plan a vulnerability assessment and penetration test for a network.
CO2: execute a penetration test using standard hacking tools in an ethical manner.
CO3: examine how social engineering can be done by attacker to gain access of useful & sensitive information about the confidential data.

LIST OF EXERCISES

1. Setup a honey pot and monitor the honey pot on network
2. Write a script or code to demonstrate SQL injection attacks
3. Create a social networking website login page using phishing techniques
4. Write a code to demonstrate DoS attacks
5. Install rootkits and study variety of options
6. Study of Techniques uses for Web Based Password Capturing.
7. Install jcrypt tool (or any other equivalent) and demonstrate Asymmetric, Symmetric Crypto algorithm, Hash and Digital/PKI signatures
8. Implement Passive scanning, active scanning, session hizaking, cookies extraction using Burp suit tool

P: 30; TOTAL: 30 PERIODS

23IC28E PENETRATION TESTING AND VULNERABILITY ASSESSMENT LABORATORY **L T P C**
0 0 4 2

COURSE OUTCOMES

CO1: Identify and analyses the stages an ethical hacker requires to take in order to compromise a target system.
CO2: Critically evaluate security techniques used to protect system and user data in windows and web-based forum.
CO3: Determine the type of attack used and pinpoint exploit code in network traffic.

LIST OF EXPERIMENTS

1. Scan the network for Windows machines in local network and virtual network.
2. Identify the open ports and firewall rules setup.
3. Use password guessing tools to guess a password. Use password strengthening tools to strengthen the password. Try guessing the password and tabulate the enhanced difficulty due to length of password and addition of special characters.
4. Extract password hashes from Windows machine. Use a password extraction tool, using word list, single crack or external mode to recover the password. Increase the complexity of the password and determine the point at which the cracking tool fails.
5. Cracking Linux passwords.
6. Experiments on SQL injections.
7. Experiments on Wireless DoS Attacks.
8. Prevention against Cross Site Scripting Attack.
9. Malwares Working and Detection
10. Networking Attacks and Security.
11. Web Server Attacks and Security
12. File upload vulnerability on social engineering.

P: 30; TOTAL: 30 PERIODS

23IC29E MALWARE ANALYSIS LABORATORY **L T P C**
0 0 4 2

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: Develop an insight to fundamentals of malware analysis for malware detection.
CO2: Implement tools and techniques of malware analysis.

LIST OF EXERCISES

1. Install and configure a virtual machine for malware analysis.
2. Execute a malware sample in a controlled environment and observe its behavior using tools like Process Monitor, Wireshark, or API monitors.
3. Use antivirus or signature-based detection tools to identify known malware patterns.
4. Analyze malware code structure, functions, and algorithms in-depth using advanced disassembly techniques.
5. Use tools like Volatility to analyze memory dumps and Identify malware artifacts in memory.
6. Analyze malware samples using techniques that attempt to evade analysis.

P: 30; TOTAL: 30 PERIODS

23IC30E WEB APPLICATION SECURITY LABORATORY **L T P C**
0 0 4 2

COURSE OUTCOMES

CO1: apply appropriate tool to identify vulnerabilities in web application
CO2: use suitable security techniques to prevent web application from attacks

LIST OF EXERCISES:

1. Install Burp Suite to do following vulnerabilities:
    - SQL injection
    - cross-site scripting (XSS)
2. Apply OWASP ZAP tool to identify the vulnerabilities in web application.
3. Attack the website using Social Engineering method
4. Apply several vulnerability scanners to find security flaws in web applications with the Burp suite tool.
5. Implementation of Comodo tool to prevent Web attacks vulnerabilities
6. Monitor the security flaws in web application using OpenVas.
7. Install wireshark and explore the various protocols
    - Analyze the difference between HTTP vs HTTPS
    - Analyze the various security mechanisms embedded with different protocols.

P: 30; TOTAL: 30 PERIODS

23IC31E	**MULTIMEDIA SECURITY LABORATORY**	**L T P C** **0 0 4 2**

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: solve practical problems related to the secure transmission, authentication, and protection of multimedia content.

CO2: analyze multimedia file systems to uncover evidence, including deleted files, hidden content, and file metadata.

LIST OF EXPERIMENTS

1. Implement a basic image watermarking algorithm using a programming language like Python or MATLAB.
2. Develop a simple audio encryption algorithm using techniques like frequency domain transformations.
3. Create a video authentication system using digital signatures or hash functions.
4. Implement a steganographic algorithm to hide text or an image within another image.
5. Design a simple biometric authentication system using facial recognition or fingerprint recognition.
6. Simulate a digital forensics investigation on multimedia data.
7. Implement basic access control mechanisms and analyze their effectiveness.

SOFTWARE REQUIREMENTS:

- MATLAB
- Audacity, Python with SciPy
- FFmpeg, OpenCV
- Steghide, OpenStego

P: 30; TOTAL: 30 PERIODS

23AC01E **TECHNICAL REPORT WRITING** **L T P C**
2 0 0 2

COURSE OUTCOMES

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

CO1: Enhance the knowledge of the research objectives and research process
CO2: Develop the level of readability for formulating rationale and improve writing skills
CO3: Formulate suitable sentences and key words for the research paper
CO4: Develop the skill of chapterisation and research writing
CO5: Interpretation of data through various strategies
CO 6: Implementation of basic rules and methods of citation

INTRODUCTION TO RESEARCH **5**

Research – Writing Definitions – Framing Objectives – Research process - Formulating Research problem – Technical terms and extended definition - Breaking up long sentences--structuring paragraphs and sentences - being concise and removing redundancy avoiding ambiguity and vagueness.

IDENTIFICATION & COLLECTION OF SOURCES **5**

Preparing manuscript – Skimming and Scanning – Review of literature- Identifying the problem - writing problem statements – writing hypothesis- Formulating Rationale – Research Design - linking phrases – Observation and Interview method – Framing Questionnaire – Case study

WRITING AND DRAFTING ABSTRACT **5**

Processing and data analysis – Identifying threats and challenges to Good Research - key skills needed to write a title - writing abstracts writing key words and introduction- Introductory phrases - Clarity in imperative sentences instruction writing – useful phrases to draft a perfect paper

CHAPTERISATION **5**

Main divisions and Subdivisions – Paragraph writing - coherence - Highlighting the findings - Analyzing Data collection - hedging and criticizing sections - Topic sentence --Paraphrasing and framing key points – Suitable section wise headings

INTERPRETATION OF DATA **5**

Non-verbal interpretation – Interpretation of Data - Abbreviations – Symbols Tables – graphs – charts - deriving result – Phrases used to Compare and Contrast -result and discussion-- skills needed to write the conclusions – avoiding common mistakes.

BIBLIOGRAPHY **5**

Citation methods – Writing Foot note – End note - bibliography – citation rules Basic reference format - plagiarism – acknowledgement – IEEE Research format – Research review Research paper Publication

L: 30; TOTAL: 30 PERIODS

REFERENCES

1. Brent, Doug. Reading as Rhetorical Invention: Knowledge, Persuasion, and the Teaching of Research-based Writing. Urbana, National Council of Teachers of English, 1992.
2. Adrian Wallwork, English for Writing Research Papers, Springer New York Dordrecht, 2016
3. Robert A. Day and Barbara Gastel, How to Write and Publish a Scientific Paper‖, Cambridge University Press, 7th Edition, 2012
4. Thiel, David V. Research Methods for Engineers. United Kingdom, Cambridge University Press, 2014.

23AC02E **DISASTER MANAGEMENT**

L	T	P	C
2	0	0	0

COURSE OUTCOMES

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

CO1: Learn to demonstrate a critical understanding of key concepts in disaster risk reduction and manitarian response.

CO2: Critically evaluate disaster risk reduction and humanitarian response policy and practice from multiple perspectives.

CO3: Develop an understanding of standards of humanitarian response and practical relevance in specific types of disasters and conflict situations.

CO4. Critically understand the strengths and weaknesses of disaster management approaches, planning and programming in different countries, particularly their home country or the countries they work in.

INTRODUCTION **4**

Disaster: Definition- Factors and Significance- Difference Between Hazard and Disaster- Natural and Manmade Disasters: Difference-Nature- Types And Magnitude.

REPERCUSSIONS OF DISASTERS AND HAZARDS **6**

Economic Damage: Loss Of Human And Animal Life, Destruction Of Ecosystem-Natural Disasters: Earthquakes, Volcanisms, Cyclones, Tsunamis, Floods, Droughts and Famines, Landslides and Avalanches- Man-made disaster- Nuclear Reactor Meltdown, Industrial Accidents, Oil Slicks And Spills, Outbreaks Of Disease And Epidemics, War And Conflicts.

DISASTER PRONE AREAS IN INDIA **6**

Study of Seismic Zones: Areas Prone To Floods And Droughts-Landslides and Avalanches Areas Prone To Cyclonic And Coastal Hazards With Special Reference To Tsunami- Post Disaster Diseases and Epidemics.

DISASTER PREPAREDNESS AND MANAGEMENT **6**

Preparedness: Monitoring Of Phenomena Triggering A Disaster Or Hazard-Evaluation Of Risk Application Of Remote Sensing- Data from Meteorological and other Agencies'-Media Reports Governmental and Community Preparedness.

RISK ASSESSMENT AND DISASTER MITIGATION **8**

Disaster Risk: Concept and Elements- Disaster Risk Reduction- Global and National Disaster Risk Situation-Techniques of Risk Assessment-Global Co-Operation In Risk Assessment and Warning, People's Participation In Risk Assessment- Strategies for Survival. Meaning: Concept and Strategies Of Disaster Mitigation-Emerging Trends In Mitigation-Structural Mitigation and Non-Structural Mitigation-Programs of Disaster Mitigation In India.

L: 30; TOTAL: 30 PERIODS

REFERENCES

1. Singhal J.P. —Disaster Managementǁ, Laxmi Publications, ISBN-10: 9380386427 ISBN-13: 978-9380386423, 2010
2. Tushar Bhattacharya, —Disaster Science and Managementǁ, McGraw Hill India Education Pvt. Ltd., ISBN-10: 1259007367, ISBN-13: 978-125900736, 2012.
3. Gupta Anil K, Sreeja S. Nair, "Environmental Knowledge for Disaster Risk Management", NIDM, New Delhi, 2011.
4. Kapur Anu, "Vulnerable India: A Geographical Study of Disasters", IIAS and Sage Publishers, New Delhi, 2010.

5. National Disaster Management Plan, 2018, https://ndma.gov.in/images/pdf/NDMP-2018-Revised-Draft-1-2018OCT16-A.pdf
6. National Disaster Management Authority, Government of India, 2018, https://ndma.gov.in/images/pdf/Draft-Guidelines-thunderstorm-final.pdf

23AC03E SANSKRIT FOR TECHNICAL KNOWLEDGE L T P C
2 0 0 0

COURSE OUTCOMES

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

CO1: Learn the Sanskrit sources of technical knowledge
CO2: Drawing their attention to a different dimension of Sanskrit literary tradition
CO3: Create awareness of the contemporary relevance of the Sanskrit sources of traditional wisdom

INTRODUCTION 7

Scope and meaning of study of technical literature in Sanskrit. Different disciplines-interdisciplinary approach-dimensions-contemporary relevance- important works in this direction-scientific methodology in ancient India.

AYURVEDA 7

Beginnings of Ayurveda in Atharvaveda-Ayurvedic literature-basic principles of Ayurveda-Pancabhutasiddhanta-Tridosasiddhanta-eight anga-s of Ayurveda- Rasacikitsa-contribution of Kerala to Ayurveda

ASTRONOMY AND MATHEMATICS 8

Major texts in Vedic and classical period-Vedangajyotisa-Sulbasutra-s-Aryabhatiya- Aryabhata's contribution-Varahamihira-Brahmagupta-Lalla-etc. Suryasiddhanta- Kerala school Parahita and drk systems-Later astronomical works commentaries.

VASTUSASTRA AND ARTHASASTRA 8

Principles of Vastusastra-Basic texts-Vastuvidya and Ecology-Iconography and sculpture-Kerala tradition of Vastusastra. Arthasastra, a historical and sociaological perspective-structure and contents of the text-emphasis to aspects of agriculture and architecture.

L: 30; TOTAL: 30 PERIODS

REFERENCES

1. Ramakrishna Mission Institute ,"Cultural Heritage of India", (Vol. i and iii), Calcutta, 2010
2. Dr.P.C. Muraleemadhavan and Dr.N.K.Sundareswaran," Sanskrit in Technological Age,(Ed.)", New Bharatiya Book Corporation, Delhi, 2006
3. https://sanskritdocuments.org/articles/ScienceTechSanskritAncientIndiaMGPrasad.pdf
4. http://www.vedanta.gr/wp-content/uploads/2012/03/3_GlossaryOfCommonSanskrit Terms.pdf

23AC04E VALUE EDUCATION L T P C
2 0 0 0

COURSE OUTCOMES

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

CO1: Understand the need of values and its classification in contemporary society
CO2: Become aware of role of education in building value as dynamic social reality.

CO3: Know the importance of value education towards personal, national and global development.

10

Values and self-development –Social values and individual attitudes- Work ethics- Indian vision of humanism-Moral and non- moral valuation- Standards and principles-Value judgements.
Importance of cultivation of values-Sense of duty- Devotion- Self-reliance- Confidence-Concentration -Truthfulness-Cleanliness- Honesty- Humanity- Power of faith- National Unity-Patriotism-Love for nature- Discipline.

10

Personality and Behavior Development - Soul and Scientific attitude- Positive Thinking -Integrity and discipline-Punctuality- Love and Kindness-Avoid fault Thinking-Free from anger- Dignity of labour-Universal brotherhood and religious tolerance-True friendship-Happiness Vs suffering- love for truth-Aware of self-destructive habits-Association and Cooperation- Doing best for saving nature.

10

Character and Competence –Holy books vs Blind faith- Self management and Good health-Science of reincarnation- Equality- Nonviolence- Humility-Role of Women- All religions and same message-Mind your Mind-Self-control-Honesty- Studying effectively.

L: 30; TOTAL: 30 PERIODS

REFERENCES

1. Sharma, S.P., "Moral and Value Education: Principles and Practices", Kanishka publishers, 2013.
2. Kiruba Charles & V.Arul Selvi.," Value Education", Neelkamal Publications, New Delhi, 2012.
3. Passi, B.K. and Singh, P.,"Value Education", National Psychological Corporation, Agra. 2004.
4. http://cbseportal.com/exam/e-books/download-free-ncert-e-book-education-for-values-in-school-a-framework/
5. http://cbseacademic.in/web_material/ValueEdu/Value%20Education%20Kits.pdf

23AC05E CONSTITUTION OF INDIA L T P C
2 0 0 0

COURSE OUTCOMES

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

CO1: understand the premises informing the twin themes of liberty and freedom from a civil rights perspective.

CO2: address the growth of Indian opinion regarding modern Indian intellectuals constitutional role and entitlement to civil and economic rights as well as the emergence of nationhood in the early years of Indian nationalism.

CO3: address the role of socialism in India after the commencement of the Bolshevik Revolution in 1917 and its impact on the initial drafting of the Indian Constitution.

HISTORY AND PHILOSOPHY OF INDIAN CONSTITUTION 6

History-Drafting Committee, (Composition & Working). - Preamble- Salient Features.

CONTOURS OF CONSTITUTIONAL RIGHTS & DUTIES 6

Fundamental Rights - Right to Equality-Right to Freedom - Right against Exploitation - Right to Freedom of Religion - Cultural and Educational Rights - Right to Constitutional Remedies - Directive Principles of State Policy- Fundamental Duties.

ORGANS OF GOVERNANCE **6**

Parliament- Composition-Qualifications and Disqualifications- Powers and Functions- Executive-President-Governor-Council of Ministers- Judiciary- Appointment and Transfer of Judges-Qualifications-Powers and Functions**.**

LOCAL ADMINISTRATION **6**

District's Administration head: Role and Importance- Municipalities: Introduction, Mayor and role of Elected Representative-CEO of Municipal Corporation-Pachayati raj: Introduction, PRI:ZilaPachayat- Elected officials and their roles,-CEO ZilaPachayat: Position and role- Block level: Organizational Hierarchy (Different departments)-Village level: Role of Elected and Appointed officials- Importance of grass root democracy.

ELECTION COMMISSION **6**

Election Commission: Role and Functioning -Chief Election Commissioner and Election Commissioners-State Election Commission: Role and Functioning.-Institute and Bodies for the welfare of SC/ST/OBC and women.

L: 30; TOTAL: 30 PERIODS

REFERENCES

1. Subhash .C, kashyap "Our Constitution", 5th Edition, 2017
2. www.ieagreements.org/IEA-Grad-Attr-Prof-Competencies.pdf
3. The Constitution of India, 1950 (Bare Act), Government Publication.
4. Dr. S. N. Busi, Dr. B. R. Ambedkar framing of Indian Constitution, 1st Edition, 2015.
5. M. P. Jain, Indian Constitution Law, 7th Edn., Lexis Nexis, 2014.
6. D.D. Basu, Introduction to the Constitution of India, Lexis Nexis, 2015.

23AC06E **PEDAGOGY STUDIES** **L T P C**
2 0 0 0

COURSE OUTCOMES

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

CO1: Describe the pedagogical practices used by teachers in formal and informal classrooms

CO2: Understand the effectiveness of these pedagogical practices, in what conditions, and with what population of learners

CO3: Analyze how teacher education (curriculum and practicum) and the school curriculum with guidance materials support effective pedagogy

INTRODUCTION AND METHODOLOGY **8**

Aims and rationale, Policy background, Conceptual framework and terminology-Theories of learning, Curriculum, Teacher education.Conceptual framework, Research questions**.** Overview of methodology and Searching. Thematic overview- Pedagogical practices are being used by teachers in formal and informal classrooms in developing countries- Curriculum- Teacher education.

EFFECTIVENESS OF PEDAGOGICAL PRACTICES **8**

Evidence on the effectiveness of pedagogical practices-Methodology for the in depth stage: quality assessment of included studies- How can teacher education (curriculum and practicum) and the school curriculum and guidance materials best support effective pedagogy- Theory of change-Strength and nature of the body of evidence for effective pedagogical Practices- Pedagogic theory and pedagogical approaches- Teachers attitudes and beliefs and Pedagogic strategies.

PROFESSIONAL DEVELOPMENT **7**

Alignment with classroom practices and follow-up support- Peer support-Support from the head teacher and the community-Curriculum and assessment-Barriers to learning: limited resources and large class sizes.

RESEARCH GAPS AND FUTURE DIRECTIONS **7**

Research design – Contexts – Pedagogy - Teacher education - Curriculum and assessment - Dissemination and research impact.

L: 30; TOTAL: 30 PERIODS

REFERENCES

1. Dr.S.K.Bhatia and Dr.Sonia Jindal, “A Text Book of Curriculum, Pedagogy and Evaluation”, Paragon International Publications, 2016.
2. Ackers J, Hardman F Classroom interaction in Kenyan primary schools, Compare, 31 (2):245-261, 2001.
3. Agrawal M, "Curricular reform in schools: The importance of evaluation", Journal of Curriculum Studies, 36 (3): 361-379, 2004.
4. Akyeampong K, "Teacher training in Ghana - does it count?", Multi-site teacher education research project (MUSTER) country report 1. London: DFID, 2003.
5. Akyeampong K, Lussier K, Pryor J, Westbrook J, "Improving teaching and learning of basic maths and reading in Africa: Does teacher preparation count?", International Journal Educational Development, 33 (3): 272–282,2013.
6. Alexander RJ,"Culture and pedagogy: International comparisons in primary education", Oxford and Boston: Blackwell, 2001.
7. Chavan M, "Read India: A mass scale, rapid, ‘learning to read’", campaign, 2003.
8. www.pratham.org/images/resource%20working%20paper%202.pdf.

23AC07E STRESS MANAGEMENT BY YOGA **L T P C**
2 0 0 0

COURSE OUTCOMES

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

CO1: achieve overall health of body and mind

CO2: overcome stress

INTRODUCTION **10**

Introduction to Stress-Concept of Stress-Solutions through Mandukya karika - Relaxation and stimulation combined as the core for stress management-Practice of Stimulation and relaxation.

ASAN AND PRANAYAM **10**

Definitions of Eight parts of yoga. (Ashtanga)-Various yoga poses and their benefits for mind & body-Regularization of breathing techniques and its effects-Types of pranayam.

YOGA AND STRESS MANAGEMENT **10**

Concepts and Techniques of Stress Management in Ashtanga Yoga of Patanjali - specific practices for stress management-breathe awareness.

L: 30; TOTAL: 30 PERIODS

REFERENCES

1. Swami Vivekananda, Advaita Ashrama ,“Rajayoga or conquering the Internal Nature”, 2016.

2. K.N.Udupa**,** **"**Stress and Its Management by Yoga", Edited by R.C.Prasad, Motilal Banarashidass Publishers, Delhi, 2010.
3. Lisa Shea,"Yoga for Stress Relief and Forgiveness", Kindle Edition, 2015.
4. BKS Iyengar, "Yoga: The path to Holstic Health", DK Publication, 2019
5. https://www.longdom.org/open-access/stress-and-yoga-2157-7595.1000109.pdf

23AC08E **PERSONALITY DEVELOPMENT THROUGH LIFE ENLIGHTENMENT SKILLS** **L T P C 2 0 0 0**

COURSE OUTCOMES

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

CO1: learn to achieve the highest goal happily
CO2: become a person with stable mind, pleasing personality and determination (K1)
CO3: awaken wisdom in students

INTRODUCTION TO PERSONALITY DEVELOPMENT **10**

The concept of personality - Dimensions of personality – Theories of Freud & Erickson- Significance of personality development. The concept of success and failure: What is success? - Hurdles in achieving success - Overcoming hurdles - Factors responsible for success – What is failure - Causes of failure-SWOT analysis.

LIFE ENLIGHTENMENT SKILLS **10**

Neetisatakam-Holistic development of personality, Verses 19,20,21,22 (wisdom), Verses 29,31,32 (pride & heroism), Verses 26,28,63,65 (virtue), Verses 52,53,59 (dont's), Verses 71,73,75,78 (do's).Approach to day to day work and duties, Shrimad Bhagwad Geeta, Chapter 2-Verses 41, 47,48, Chapter 3 Verses 13, 21, 27, 35, Chapter 6 Verses 5,13,17, 23, 35, Chapter 18 Verses 45, 46, 48.

SHRIMAD BHAGWAD GEETA STATEMENTS **10**

Statements of basic knowledge, Shrimad Bhagwad Geeta: Chapter2 Verses 56, 62, 68, Chapter 12 Verses 13, 14, 15, 16,17, 18, Personality of Role model. Shrimad Bhagwad Geeta, Chapter2 Verses 17, Chapter3 Verses 36, 37, 42, Chapter4 Verses 18, 38,39, Chapter18 Verses 37,38,63

L: 30; TOTAL: 30 PERIODS

REFERENCES

1. Swami Swarupananda Advaita Ashram, "Srimad Bhagavad Gita", Publication Department, Kolkata.
2. P.Gopinath, Rashtriya Sanskrit Sansthanam, "Bhartrihari's Three Satakam (Niti-sringar-vairagya) ", New Delhi.