NATIONAL INSTITUTE OF ELECTRONICS AND INFORMATION TECHNOLOGY

DEEMED TO BE UNIVERSITY UNDER DISTINCT CATEGORY

(AN AUTONOMOUS INSTITUTION UNDER MINISTRY OF ELECTRONICS & IT, GOVT. OF INDIA)

Curriculum and Syllabi for

M.Tech - Cyber Forensics and Information Security

(2025-26 Scheme)

Main Campus at Ropar and Constituent Units at Aizawl, Agartala, Aurangabad, Calicut, Gorakhpur, Imphal, Itanagar, Kekri, Kohima, Patna and Srinagar

Vision

To develop highly skilled professionals equipped with advanced knowledge and practical expertise in cyber forensics and information security, empowering them to tackle evolving cyber threats, safeguard digital assets, and lead innovations in securing the digital ecosystem. The program aspires to bridge the global skill gap by fostering proficiency in emerging technologies and aligning with industry and legislative demands for robust cybersecurity solutions

Mission

To provide a strong foundation in cyber forensic and information security through the integration of advanced electronic components, fundamental cybersecurity principles, and cutting-edge technologies. The program aims to equip students with the knowledge and skills required to address modern cyber threats, ensure data integrity, and contribute to the development of secure digital infrastructures.

Program Education Objectives

Post Graduates of the M.Tech(CFIS) program will be able to:
1.Attain advanced education, equipped with a deep understanding enriched by both academic and industrial skill sets.
2.Achieve excellence in one's professional journey by mastering the ability to offer effective solutions to Information Technology challenges.
3.Demonstrate leadership qualities and contribute actively within teams, serving as catalysts for change and innovation in organizations focused on product design and manufacturing.
4.Showcase flexible and nimble skills in the specialized field of Information Science & Engineering to effectively tackle both technical and managerial challenges.

Program Outcomes

1.An ability to independently carry out research /investigation and development work to solve practical problems.
2.An ability to write and present a substantial technical report/document.
3.An ability to demonstrate a degree of mastery over the area as per the specialization of the program An ability to use modern tools for engineering design problems, analyze the performance and optimize the systems-level approaches.
4.An ability to engage in independent and life-long learning in the context of technological change and industrial demands. Rephrase above outcomes

Program Specific Outcomes

1.Understand the evolution of cybersecurity measures and their role in addressing the growing complexity of digital threats.
2.Utilize essential tools and technologies to support forensic investigations and secure information assets effectively

CATEGORY WISE CREDIT DISTRIBUTION

Category	Category Code	Credits
Skill / Employment Enhancement Courses (Project/Internship/Seminar/Dissertation/Research)	EE	36
Audit Courses (without grade or credit)	AU	0
Open Elective Courses	OE	8
Professional Elective Courses	PE	16
Program Core Courses	PC	20
Total Credits (Common track)		**80**

EVALUATION AND ASSESSMENT

1. Performance of a student in a semester shall be evaluated through continuous Class assessment, Tutorial/Lab assessment, Mid-Semester Examination (MSE) and End-Semester Examination (ESE). Both the MSE and ESE shall be the University examination and will be conducted as notified by the Controller of Examinations (CoE) of the University.

2. The continuous assessment shall be based on assignments, tutorials, paper presentation / quizzes/ viva-voce / flipped classes, lab work / projects / fieldwork and attendance, etc.

3. The MSE/ESE shall be comprising of written papers.

4. The overall assessment of the students will be done as per the following scheme:

S. No.	Assessment Type	Marks Weightage
1.	Mid Semester Examination	20
2.	End Semester Examination	40
3.	Continuous Assessment - Practical /Lab/ Tutorial	25
4.	Continuous Assessment - Theory	15
Total		**100**

For more details, please refer the applicable ordinance for this programme and Assessment SOPs.

CURRICULUM

Semester 1						
Semester Code	**Course Code**	**Course Title**	**L**	**T**	**P**	**Cr**
PC-MTECFI-101	DASH250077	Mathematics for Information Security and Cyber Forensics	3	1	0	4
PC-MTECFI-102	DCSE250004	Advanced Data Structures and Algorithms	3	0	2	4
PE-MTECFI-103	Elective	Program Elective				4
OE-MTECFI-104	Elective	Open Elective				4
PC-MTECFI-105	DASH250095	Research Methodology and IPR	3	1	0	4
AU-MTECFI-106	Elective	Audit Elective				0

Semester 2						
Semester Code	**Course Code**	**Course Title**	**L**	**T**	**P**	**Cr**
PC-MTECFI-201	DCSE250065	Digital Forensics & Cyber Crime Investigation	3	0	2	4
PC-MTECFI-202	DCSA250047	Malware Analysis	3	0	2	4
PE-MTECFI-203	Elective	Program Elective				4
PE-MTECFI-204	Elective	Program Elective				4
AU-MTECFI-205	Elective	Audit Elective				0
EE-MTECFI-206	EE	Mini project with Seminar				4

Semester 3						
Semester Code	**Course Code**	**Course Title**	**L**	**T**	**P**	**Cr**
PE-MTECFI-301	Elective	Program Elective				4
OE-MTECFI-302	Elective	Open Elective				4
EE-MTECFI-303	EE	Dissertation-I				14

Semester 4						
Semester Code	**Course Code**	**Course Title**	**L**	**T**	**P**	**Cr**
EE-MTECFI-401	EE	Dissertation-II				18

Elective Courses

Elective Courses for PE Category						
Course Code	**Course Title**	**L**	**T**	**P**	**Cr**	**For Sem./Code**
DCSA250005	Applied Cryptography	3	1	0	4	
DCSA250008	Biometrics	3	1	0	4	
DCSA250009	Blockchain Technology	3	1	0	4	
DCSA250021	Cyber Law	3	1	0	4	
DCSA250033	Image Forensics and Security	3	0	2	4	
DCSA250035	Information Security Audit	3	0	2	4	
DCSE250023	Cloud Computing Security	3	1	0	4	
DCSE250049	Data Privacy	3	0	2	4	
DCSE250072	Edge Computing	3	1	0	4	
DCSE250073	Ethical Hacking	2	1	2	4	
DCSE250075	Forensic Psychology	3	1	0	4	
DCSE250104	Operating Systems Security	3	0	2	4	
DCSE250125	Web and Database Security	3	1	0	4	
DOAI250017	Data Analytics for Fraud Detection	3	0	2	4	
DOEE250124	IOT and its Applications	3	1	0	4	

Elective Courses for OE Category
Students may opt courses under MOOC, NPTEL, SWAYAM, NSQF/NCVET aligned courses or other relevant technical subjects not included in their core curriculum. The exercise of option shall be subject to the Course Schedule of the respective Constituent Unit, the credit requirements and availability of seats. Guidelines for choosing MOOC/Online courses are given separately and shall have to be adhered to.

Elective Courses for AU (Audit) Category					
Course Code	**Course Title**	**L**	**T**	**P**	**Cr**
DASH240027	Disaster Management	2	0	0	0
DASH240047	English for Research Paper Writing	2	0	0	0
DASH240052	Environmental Science	3	0	0	0
DASH240085	Pedagogy Studies	2	0	0	0
DASH240086	Personality Development through Life Enlightenment Skills	2	0	0	0
DASH240097	Sanskrit for Technical Knowledge	2	0	0	0
DASH240103	Stress Management by Yoga	2	0	0	0
DASH240104	Technical Presentation and Report Writing	0	0	2	0
DASH240106	Value Education	2	0	0	0
DASH240124	Constitution of India - AU	2	0	0	0
DASH250023	Constitution of India	2	1	0	0
DASH250027	Disaster Management	3	0	0	0
DASH250034	Energy and Environmental Engineering	3	0	0	0

DASH250047	English for Research Paper Writing	2	0	0	0
DASH250054	Essence of Indian Knowledge and Tradition	2	0	0	0
DASH250085	Pedagogy Studies	2	0	0	0
DASH250086	Personality Development	2	0	0	0
DASH250097	Sanskrit for Technical Knowledge	3	0	0	0
DASH250103	Stress Management by Yoga	3	0	0	0
DASH250106	Value Education	2	0	0	0
DASH250117	Innovative Thinking and Entrepreneurship Skills	1	0	0	0
DASH250118	Intellectual Property Rights	2	0	0	0
DCSA240080	Training on Computer Networking	0	0	2	0
DCSA240304	Lab Based on Statistical Package	0	0	2	0
Any other Scheduled Course as per the Course Schedule of the respective Constituent Unit can also be chosen, subject to availability of seats. However, there shall be no assessment and grading for the course chosen as Audit Course.					

The choice of all type of Electives available shall be as per the Course Schedule of the respective Constituent Unit.

Guidelines for Massive Open Online Courses (MOOC) / approved Online Courses

1. Relevant Swayam, MOOC, NPTEL, NIELIT NSQF and any other online courses approved by UGC/AICTE shall also be allowed as Open Electives(OE).

2. One credit of MOOC course should be minimum of 30 hours.

3. A student can choose any approved online course as Open Elective, subject to minimum credit requirements.

4. The students willing to opt OE under MOOC in their next semester, will submit their request to the MOOC Coordinator at their respective campus.

5. Once approved, the campus shall display the list of accepted courses.

6. The student has to submit certificate issued by the institution offering the MOOCs course, along with the number of credits and grades, to get credits transferred into his/her marks certificate issued by NDU.

7. The transfer of credits shall be as adopted by NDU.

Detailed Syllabus

Course Code	Course Name	L	T	P	Cr
DASH250077	Mathematics for Information Security and Cyber Forensics	3	1	0	4

Course Outcomes:

CO1: Apply number theory concepts such as modular arithmetic, prime factorization, and congruences to design and analyze cryptographic algorithms.
CO2: Demonstrate the use of algebraic structures, finite fields, and group theory in developing secure communication and error detecting codes.
CO3: Utilize probability, statistics, and combinatorics to model security attacks, risk analysis, and forensic investigation.
CO4: Analyze linear algebraic methods including matrices, vector spaces, and transformations for cryptographic primitives, coding, and data authentication.
CO5: Evaluate mathematical techniques in hashing, digital signatures, elliptic curve cryptography, and information-theoretic security to solve real-world cybersecurity problems

Module 1:

Number Theory for Cryptography (9 Hours)
Prime numbers, divisibility, GCD, Euclidean algorithm, modular arithmetic, congruences, Fermat's Little Theorem, Euler's theorem, Chinese Remainder Theorem, applications in RSA, Diffie–Hellman, and modular exponentiation.

Module 2:

Algebraic Structures and Finite Fields (9 Hours)
Groups, rings, and fields; finite fields (GF(p), GF(2^n)); polynomial arithmetic over finite fields; applications in AES, elliptic curve cryptography, and error-correcting codes.

Module 3:

Probability, Statistics, and Combinatorics in Security (9 Hours)
Probability spaces, conditional probability, Bayes' theorem, random variables and distributions (Binomial, Poisson, Gaussian), entropy and uncertainty, birthday paradox, hash collision probability, applications in key management, intrusion detection, and forensic analysis.

Module 4:

Linear Algebra for Cryptography and Coding (9 Hours)
Vectors, matrices, linear transformations, determinants, eigenvalues/eigenvectors, matrix factorization, applications in Hill cipher, error-detecting codes, data hiding, and steganography.

Module 5:

Advanced Mathematical Tools for Information Security (9 Hours)
Elliptic curve cryptography (ECC): basics of elliptic curves over finite fields; digital signatures, message authentication codes (MACs); hash functions and their mathematical foundations; lattice-based cryptography (basics); information-theoretic security concepts.

Labs / Practicals:

N/A

References:

1. Babu Ram – Discrete Mathematics, Pearson / Vikas Publishing
2. Dr. S. Balakrishnan – Discrete Mathematics, Laxmi Publications
3. S.C. Gupta and V.K. Kapoor – Fundamentals of Mathematical Statistics, Sultan Chand & Sons
4. N.G. Das – Statistical Methods (Volumes I & II combined), McGraw Hill Education India
5. A.M. Goon, M.K. Gupta, B. Dasgupta – Fundamentals of Statistics, World Press
6. B.S. Grewal – Higher Engineering Mathematics, Khanna Publishers
7. N.P. Bali and Manish Goyal – A Textbook of Engineering Mathematics, Laxmi Publications
8. Rosen, Kenneth H. – Discrete Mathematics and its Applications, McGraw Hill.

Course Code	Course Name	L	T	P	Cr
DCSE250004	Advanced Data Structures and Algorithms	3	0	2	4

Course Outcomes:

CO1: Analyze the performance of basic data structures and sorting/searching techniques.
CO2: Implement and apply advanced trees, heaps, and hash tables to solve complex problems.
CO3: Solve problems using graph algorithms and greedy strategies.
CO4: Design algorithms using divide and conquer, backtracking, and dynamic programming.
CO5: Develop efficient and scalable solutions using appropriate algorithmic techniques.

Module 1:

Review of Fundamental Concepts
Pointers and Dynamic Memory Allocation, Arrays, Dynamically Allocated Arrays, Structures, Algorithm Specification, Data Abstraction, Performance Analysis, Performance Measurement, Time and space complexity

Module 2:

Basic Data Structures and Advanced Trees
Stacks, Queues, Linked Lists, Hash Tables, Searching and Sorting Techniques: Linear Search, Bubble Sort, Selection Sort, Insertion Sort, Binary Trees, Binary Tree Traversals, Applications of Binary Trees, Threaded Binary Trees, Binary Search Trees, Advanced Trees: AVL Trees: Rotations, insertion and deletion, Red-Black Trees, Splay Trees, B Trees, B+ Trees, Binary Heap: Min/Max heap operations, Priority Queue applications.

Module 3:

Divide and Conquer, Backtracking, String Matching algorithms
Merge Sort, Quick Sort, Binary Search, Backtracking: N-Queens, Graph Coloring, String matching algorithms: KMP, Rabin-Karp

Module 4:

Graph Algorithms
Graph Representations: Adjacency list, Adjacency Matrix, BFS, DFS, Shortest Path: Dijkstra’s, Greedy algorithms: Activity Selection, Huffman Coding Minimum Spanning Tree: Prim’s and Kruskal’s Algorithms

Module 5:

Dynamic Programming
Basic concepts: Overlapping subproblems, optimal substructure, 0/1 Knapsack, Longest Common Subsequence, Matrix Chain Multiplication

Labs / Practicals:

Preparing

References:

1. "Introduction to Algorithms (Fourth Edition)" by Thomas H. Cormen, Charles Eric Leiserson, Ronald Linn Rivest, Clifford Seth Stein
https://mitpress.mit.edu/9780262046305/introduction-to-algorithms

2. "A Second Course in Algorithms" by Timothy Avelin Roughgarden
https://timroughgarden.org/w16/l

3. "Algorithm Design" by Jon Michael Kleinberg and Eva Tardos
https://dl.acm.org/doi/10.5555/1051910

4. "Computational Intractability: A Guide to Algorithmic Lower Bounds" by Erik D. Demaine, William Ian Gasarch, and Mohammad Taghi Hajiaghayi
https://hardness.mit.edu/drafts/2025-02-02.pdf

5. "The Design and Analysis of Algorithms" by Dexter Campbell Kozen
https://www.cs.cornell.edu/kozen/Papers/daa.pdf

6. "The Art of Computer Programming" by Donald Ervin Knuth
https://www-cs-faculty.stanford.edu/~knuth/taocp.html

Course Code	Course Name	L	T	P	Cr
DASH250095	Research Methodology and IPR	3	1	0	4

Course Outcomes:

CO1: Understand the principles and process of research methodology.
CO2: Apply appropriate research design and data collection methods in computing projects.
CO3: Analyze and interpret qualitative and quantitative data using statistical tools.
CO4: Develop ethically sound, well-documented research or project reports conforming to academic and industrial standards.
CO5: Understand various forms of intellectual property and apply processes for protection and patent filing.

Module 1:

Introduction to Research and Research Ethics
Definition and objectives of research, types of research – fundamental, applied, exploratory, empirical, significance of research in computer applications, research ethics and integrity, plagiarism, citation styles (APA, IEEE), tools for plagiarism check.

Module 2:

Research Design and Data Collection
Research problem identification and formulation, hypothesis generation, literature review techniques, types of research design: experimental, descriptive, analytical, sampling techniques, primary and secondary data sources, survey design, case study design.

Module 3:

Data Analysis and Interpretation
Quantitative and qualitative data analysis, measures of central tendency and dispersion, t-test, ANOVA, correlation and regression, chi-square test, software tools: Excel, R, SPSS (demo-level), data visualization and result interpretation.

Module 4:

Technical Writing and Project Report Preparation
Structure of research papers and reports, abstract, introduction, literature review, methodology, results, and conclusions, referencing tools (Mendeley/Zotero), IEEE/ACM/SCI journal guidelines, thesis and dissertation formatting, proposal writing basics.

Module 5:

Intellectual Property Rights and Patent Process
Introduction to IPR: patents, copyrights, trademarks, industrial design, Indian and international patent systems (WIPO, TRIPS), criteria for patentability, patent filing process in India (IPINDIA portal), open-source licenses, patent drafting basics, IPR in software and AI innovations.

Labs / Practicals:

N/A

References:

1. C.R. Kothari & Gaurav Garg – Research Methodology: Methods and Techniques, New Age International.
2. Ranjit Kumar – Research Methodology – A Step-by-Step Guide, Sage Publications India.
3. P. Narayan – Intellectual Property Law, Eastern Book Company.
4. Neeraj Pandey & Khushdeep Dharni – Intellectual Property Rights, PHI Learning.
5. Yogesh Kumar Singh – Fundamentals of Research Methodology and Statistics, New Age International.
6. Bharat Bhushan – Research Methodology in Computer Science, Himalaya Publishing.
7. WIPO and IPIndia Manuals – Guidelines for Filing Patents in India.

Course Code	Course Name	L	T	P	Cr
DCSE250065	Digital Forensics & Cyber Crime Investigation	3	0	2	4

Course Outcomes:

CO1:Understand the languages of digital forensics,and the investigation of digital crime scene
CO2:Learn the basics of computer investigators
CO3:Become knowledgeable in the digital forensics networks and OSI layers

Module 1:

Introduction: Computer Forensics Needs, Computer forensics fundamentals, Introduction to Steps of Digital Forensics, Computer Crimes, Types of Digital forensics evidences, Legal Aspects of Digital Forensics.

Module 2:

Hardware and Software: Understanding Computer components- input and output devices, CPU, Digital Media, System software - Operating System Architecture, Application Software, File Systems, Memory organization concept, Data Storage concepts. Network: Topology, Devices, Protocols and Port, Communication media. IP Address: Types and classes.

Module 3:

Foundations: Basic Principles and methodologies for digital forensics, Design systems with forensic needs in mind. Phases of Digital Forensics. Introduction to Digital Forensics Tools, Life of a Digital Forensic Investigator. Data Acquisition: Principles of Digital Forensic Acquisition, Evidence Handling and Processing Digital Forensic Data.

Module 4:

Evidence Collection: Rules of Evidence, Jurisdictions, Techniques and standards for Preservation of Data. Evidence Analysis: OS /File System Forensics, Application Forensics, Web Forensics, Network Forensics, Mobile Device Forensics.

Module 5:

Investigation: Computer, Network, System attacks, Attack detection and investigation, Anti forensics. Case studies on File System, Network storage, Web and Mobile

Labs / Practicals:

NA

References:

1. Thomas J Holt , Adam M Bossler, Kathryn C Seigfried-Spellar, Cybercrime and Digital Forensics: An Introduction, Routledge, 2016
2. Eoghan Casey, Handbook of Digital Forensics and Investigation, Academic Press, 2017
3. Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, III Edition,
2016
4. Angus McKenzie Marshall, Digital Forensics: Digital Evidence in Criminal Investigations, Wiley- Blackwell, 2018

Course Code	Course Name	L	T	P	Cr
DCSA250047	Malware Analysis	3	0	2	4

Course Outcomes:

CO1:Understand the purpose of malware analysis
CO2:Analyze various malwares and understand the behavior of malwares in real world applications
CO3: Implement different malware analysistechniques
CO4:Identify the various tools for malware analysis.
CO5:Analyze the malware behavior in windows and android

Module 1:

Malware Analysis and Reverse Engineering, Types of Malware Analysis, Purpose of Malware Analysis Limitations of Malware Analysis, The Malware Analysis Process , Malware Classes Infectors, Network Worms, Trojan Horse Backdoors, Remote-Access Trojan, Information Stealers

Module 2:

Malware Infection Vectors, Speed, Stealth, Coverage, Shelf Life, Types of
Malware Infection Vectors, Physical Media, E-mails. Instant Messaging and Chat, Social Networking, URL Links, File Shares, Software Vulnerabilities Protective Mechanisms- The Two States of Malware, Static Malware, Dynamic Malware, Protective Mechanisms, Static Malware Protective Mechanisms, Dynamic Malware Protective Mechanisms

Module 3:

Dependency Types, Environment Dependencies, Program Dependencies, Timing Dependencies, Event Dependencies, Malware Collection- Your Own Backyard, Scan for Malicious Files, Look for Active Rootkits, Inspect Startup Programs, Inspect Running Processes, Extract Suspicious Files, The Portable Executable File-The Windows Portable Executable File, The PE File Format, Relative Virtual Address, PE Import Functions

Module 4:

The Proper Way to Handle Files- File’s Analysis Life Cycle, Transfer, Analysis, Storage, Inspecting Static Malware- Static Analysis Techniques, File Type Identification, Antivirus Detection, Protective Mechanisms Identification, PE Structure Verification

Module 5:

Static Analysis Techniques, ID Assignment-File
Type Identification, Antivirus Detection, Protective Mechanisms Identification,PE Structure Verification, Dynamic Analysis-Analyzing Host Behavior,Analyzing Network Behavior

Labs / Practicals:

1.Worm Propagation Analysis in a Controlled Lab Network
Simulate and observe how a worm spreads across networked systems in an isolated lab environment.

2.Fileless Malware Detection Using Memory Analysis
Analyze system memory dumps to identify malware that operates without writing files to disk.

3.Ransomware Sample Analysis
Examine the behavior and encryption mechanisms of a ransomware sample in a controlled setup.

4. Behavioral Analysis of Packed Malware
Execute and monitor packed malware to observe runtime behavior and identify unpacking techniques.

5.Malicious PowerShell Script Dissection

Analyze a PowerShell script used for malicious purposes to uncover its payload and execution logic.

6.Reverse Engineering an Unpacked Malware Executable
Use static analysis tools to study the code and functionality of an unpacked malware binary.

7.Adware and Spyware Activity Monitoring in Sandbox
Run adware/spyware samples in a sandbox to monitor pop-ups, tracking behavior, and data exfiltration.

8.Network-Based Malware Analysis via Packet Capture
Capture and examine network traffic generated by malware to identify C2 communication and data leaks.

9.Android APK Malware Reverse Engineering
Decompile and inspect a malicious Android APK to identify harmful permissions and embedded code.

10.Macro-Based Malware Embedded in Office Documents
Analyze a malicious document to investigate embedded macros and their impact upon execution.

11.Trojan Horse Malware Functionality Inspection
Study a trojan sample to understand its disguise mechanism and malicious actions post-installation.

12.Keylogger Identification and Payload Behavior
Detect and analyze a keylogger's logging activity and data exfiltration mechanisms.

13.Persistence Mechanisms Used by Malware
Investigate how malware maintains persistence through registry keys, startup folders, or scheduled tasks.

References:

1. Cameron H. Malin, Eoghan Casey, James M. Aquilina and Curtis W. Rose, Malware ForensicsField Guide for Windows Systems, Syngress, Elsevier, 2014
2. Ken Dunham, Saeed Abu-Nimeh, Michael Becher and Seth Fogie, Mobile Malware Attacks andDefense, Syngress, Elsevier, 2009
3. Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides byCameron H.Malin, Eoghan Casey, James M. Aquiline 1 st Edition.
4. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and MacMemory by Michael Hale Ligh, Kindle Edition

Course Code	Course Name	L	T	P	Cr
DCSA250005	Applied Cryptography	3	1	0	4

Course Outcomes:

CO1: Understand the fundamentals of number theory and algorithms.
CO2: Analyze, design and implement different cryptography protocols.
CO3: Apply the intermediate protocols for linking and distributing.
CO4: Understand various Security practices and System security standards.
CO5:Apply the various Authentication schemes to simulate different applications.

Module 1:

Number theory: Fermat"s and Euler"s theorem-Chinese remainder theorem-Euclidean algorithm- Test for primality-Discrete logarithms, Information theory: entropy, Uncertainty Complexity theory: pseudo random number generation and generators.

Module 2:

Protocol Building Blocks-Basic Protocols: key Exchange-Authentication-Authentication and Key exchange: Wide-mouth frog, Yahalom, Kerberos-Formal Analysis of Authentication and Key Exchange Protocols-Multiple Key Public Key Cryptography-Secret Splitting-Secret Sharing: Secret Sharing with Cheaters-Cryptographic protection of Databases.

Module 3:

Time stamping services, Linking protocol, Distributed Protocol-Undeniable digital signaturesProxy Signatures-Group Signatures-Fail-stop signatures-computing with encrypting data-bit commitment- Fair coin flips-one-way accumulators.

Module 4:

Zero knowledge proof, Parallel Zero Knowledge Proof, Zero Knowledge proof of identity: Chess Grandmaster Problem-Blind Signatures-Simultaneous Contract Signing-Digital certified Mail- Simultaneous Exchange of Secrets-Esoteric protocols: Secure Elections-Secure Multiparty Computation.- Digital cash.

Module 5:

Key Length: Symmetric key Length, Public Key length-Algorithm types and Modes: Electronic Code Book Mode, Block Replay, Cipher Block Chaining Mode-Using Algorithms: Choosing an Algorithm, Public Key Cryptography vs Symmetric Cryptography, Encrypting Communication Channels- Public Key Algorithms: RSA, Pohlig-Hellman, Rabin, Elliptic Curve Cryptosystems - Public Key Digital Signature Algorithms: Ghost Digital Signature Algorithm, Discrete Logarithm Signature schemes. Real World approach: IBM secret key management protocol- MITRENET,ISDN, SESAME.

Labs / Practicals:

NA

References:

1. AppliedCryptography:Protocols,AlgorithmsandsourcecodeinC,Wiley,SecondEdition- Bruce Schneier (OCT 18, 1996)
2. CryptographyandNetworkSecurityPrinciplesandpractices-WilliamStallings(Jan24,2010)
3. FoundationsofCryptography:Volume1,BasicToolsbyOdedGoldreich(Jan18,2007)
4. Encryption: High-impact Strategies- What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity... by Kevin Roebuck, Emereopty Limited, 2011.
5. Foundations of Cryptography: Volume2, Basic Applications by Oded Gold reich (Sep17,2009)

Course Code	Course Name	L	T	P	Cr
DCSA250008	Biometrics	3	1	0	4

Course Outcomes:

CO1: Understand biometric traits, image processing concepts, and error analysis for biometric system design.
CO2: Apply various filtering and edge detection techniques to enhance and analyze biometric images.
CO3: Explain biometric system components, authentication methods, and feature extraction using PCA.
CO4: Evaluate system performance using FAR/FRR, ROC/DET curves, and assess security vs. usability trade-offs.
CO5: Analyze multi-modal biometric systems, identify vulnerabilities, and apply recognition techniques for fingerprints, faces, signatures, ears, and irises.

Module 1:

Introduction of biometric traits and its aim. Image processing, pattern recognition, statistics, error types. What is image, acquisition, types. Point operations, geometric transformations. Linear interpolation, brightness correction, histogram.

Module 2:

Basic image operations: convolution, linear/non-linear filtering. Gaussian, median, min filters, gray level reduction. Special filters, enhancement filters. Edge detection, derivatives, Laplacian, unsharp masking. High-boost filtering, sharpening, edge detection steps. First and second derivatives, smoothing, thresholding, localization. Robert's, Sobel's, Prewitt methods, Laplacian of Gaussian, Zero crossing. Canny edge detection. Fourier series, DFT, inverse DFT.

Module 3:

Biometric system, authentication. Physiological and behavioral traits, biometric system properties. Application areas of biometrics. PCA, eigenvectors/values, 2D-PCA, generalization to p-dimensions. Covariance, correlation, PCA algebra, data projection.

Module 4:

Identification vs. verification, threshold, score distribution. FAR/FRR, system design issues. Positive/negative identification, authentication methods and protocols. Hypothesis testing (H_0, H_1), error types I/II. Matching score distribution, FM/FNM, ROC, DET, FAR/FRR curves. Comparing systems using ROC, EER, biometric myths. Trade-offs: security vs. convenience. Biometric selection, Zephyr charts, multi-biometric types.

Module 5:

Multi-model system verification, normalization, fusion methods. Multi-modal identification, biometric system security. System vulnerabilities: circumvention, covert acquisition. Quality control, template generation, data storage, interoperability. Signature recognition system: cropping, enhancement, matching. DWT, face detection, feature template, matching. Fingerprint recognition: enhancement, thinning, minutiae, CN number. Ear and iris recognition: image acquisition, cropping, normalization.

Labs / Practicals:

NA

References:

1. Digital Image Processing using MATLAB, By: Rafael C. Gonzalez, Richard Eugene Woods, 2nd Edition, Tata McGraw-Hill Education 2010
2. Guide to Biometrics, By: Ruud M. Bolle, Sharath Pankanti, Nalini K. Ratha, Andrew W. Senior, Jonathan H. Connell, Springer 2009
3. Pattern Classification, By: Richard O. Duda, David G.Stork, Peter E. Hart, Wiley 2007

Course Code	Course Name	L	T	P	Cr
DCSA250009	Blockchain Technology	3	1	0	4

Course Outcomes:

Upon completion of the course, the learners will be able to:
CO1: Understand the concept of blockchain and its need.
CO2: Analyze methods of cryptography for application with blockchain.
CO3: Evaluate the working of blockchain.
CO4: Understand the underlying technology of transactions, blocks, proof-of-work, and consensus building.
CO5: Identify real world problems that blockchain can solve and analyze a use case.

Module 1:

Fundamentals of Blockchains Technology, The Structure of Blockchains, Blockchain Applications, The Blockchain Life Cycle, Distributed Ledger vs Centralized System, Merkel Root, Nonce Value, Hash Algorithm, and its applications.

Module 2:

Block Ciphers; Encryptions; Secret Keys; Elliptic Curve Cryptography; Hash cryptography; Encryption vs hashing; Digital Signature; Memory Hard Algorithm, Zero Knowledge Proof.

Module 3:

Introduction: Transactions, blocks, hashes, consensus, verify and confirm blocks, peer to peer networks, blocks of data in a chain, decentralization of networks, processes & workflows, cryptocurrencies, nodes, assets, consensus; types of blockchain; chain policy; working of blockchain; life of blockchain application; privacy, anonymity and security of blockchain.

Module 4:

Hyperledger: Introduction, where can Hyperledger be used, Hyperledger architecture, Hyperledger Fabric, features of Hyperledger; Open source blockchain platform technology; Tools & services; Cloud options in blockchains AWS; Azure workbench; Hyperledger console; Consensus: Proof of work, proof of stake, delegated proof of stake, proof of burn, BlocBox Protocol.

Module 5:

History; Distributed ledger; Smart contracts; Cryptocurrency; Bitcoin protocols; Mining strategy and rewards; Ethereum – construction; DAO; GHOST; Vulnerability; Attacks; Sidechain; Namecoin

Labs / Practicals:

NA

References:

1. D. Tapscott, A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, Portfolio Publishers.
2. A. Antonopoulos, Mastering Bitcoin: Programming the Open Blockchain, O'Reilly.
3. P. Champagne, The Book of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto, e53 Publishing, LLC.
4. M. Swan, Blockchain: Blueprint for a New Economy, O'Reilly.

5. R. Wattenhofer, The Science of the Blockchain, Inverted Forest Publishing.
6. R. Modi, Solidity Programming Essentials: A beginner's guide to build smart contracts for Ethereum and blockchain, Pack

Course Code	Course Name	L	T	P	Cr
DCSA250021	Cyber Law	3	1	0	4

Course Outcomes:

CO1: Collect information using network scanning
CO2: Execute a penetration test using standard hacking tools in an ethical manner
CO3: Identify legal and ethical issues related to vulnerability and penetration testing
CO4: Plan a vulnerability assessment and penetration test for a network
CO5: Identify methods to gain access to systems

Module 1:

Emergence of Cyber space. Cyber Jurisprudence, Jurisprudence and law, Doctrinal approach, Consensual approach, Real Approach, Cyber Ethics, Cyber Jurisdiction, Hierarchy of courts, Civil and criminal jurisdictions, Cyberspace-Web space, Web hosting and web Development agreement, Legal and Technological Significance of domain Names, Internet as a tool for global access.

Module 2:

Overview of IT Act, 2000, Amendments and Limitations of IT Act, Digital Signatures, Cryptographic Algorithm, Public Cryptography, Private Cryptography, Electronic Governance, Legal Recognition of Electronic Records, Legal Recognition of Digital Signature Certifying Authorities, Cyber Crime and Offences, Network Service Providers Liability, Cyber Regulations Appellate Tribunal, Penalties and Adjudication.

Module 3:

Patent Law, Trademark Law, Copyright, Software – Copyright or Patented, Domain Names and Copyright disputes, Electronic Data Base and its Protection, IT Act and Civil Procedure Code, IT Act and Criminal Procedural Code, Relevant Sections of Indian Evidence Act, Relevant Sections of Bankers Book Evidence Act.

Module 4:

Relevant Sections of Indian Penal Code, Relevant Sections of Reserve Bank of India Act, Law Relating To Employees And Internet, Alternative Dispute Resolution , Online Dispute Resolution (ODR).Evolution and development in E-commerce, paper vs paper less contracts E-Commerce models- B2B, B2C, E security.

Module 5:

Application area: Business, taxation, electronic payments, supply chain, EDI, E-markets, Emerging Trends. Case Study On Cyber Crimes: Harassment Via E-Mails, Email Spoofing (Online A Method Of Sending E-Mail Using A False Name Or E-Mail Address To Make It Appear That The E-Mail Comes From Somebody Other Than The True Sender, Cyber Pornography (Exm.MMS),Cyber- Stalking

Labs / Practicals:

NA

References:

1. K. Kumar," Cyber Laws: Intellectual property & ECommerce, Security",1st Edition, Dominant Publisher,2011.
2. Rodney D. Ryder, "Guide To Cyber Laws", Second Edition, Wadhwa And Company, New Delhi, 2007
3. Rodney D. Ryder, "Guide To Cyber Laws", Second Edition, Wadhwa And Company, New Delhi, 2007.

4. Information Security policy & implementation Issues, NIIT, PHI.
5. Vakul Sharma, "Handbook of Cyber Laws" Macmillan India Ltd, 2
nd Edition, PHI, 2003.
6. Justice Yatindra Singh, "Cyber Laws", Universal Law Publishing, 1stEdition, New Delhi, 2003.
7. Sharma, S.R., “Dimensions Of Cyber Crime”, Annual Publications Pvt. Ltd., 1
st Edition, 2004.
8. Augastine, Paul T., ”Cyber Crimes And Legal Issues”, Crescent Publishing Corporation, 2007.

Course Code	Course Name	L	T	P	Cr
DCSA250033	Image Forensics and Security	3	0	2	4

Course Outcomes:

CO1: Upon successful completion of this course,the students will get an in-depth knowledge in image and video forensics and its security techniques
CO2: Helps students to learn various types of image formation Techniques
CO3: Students will earn the Fourier Transform and Forensic image analysis
CO4: Students will gain the knowledge of statistical based forensics.
CO5: Students learn to conduct a Video Forensics & Image Security Techniques in an organized and systematic way.

Module 1:

Introduction to Image Processing, Background, Digital Image Representation, Fundamental steps in Image Processing, Elements of Digital Image Processing- Image Acquisition, Storage, Processing, Communication, Display.

Module 2:

Image formation, image compression, point processing, neighbourhood operations, image analysis. Morphological Image Processing : Dilation and Erosion, Opening and Closing, Extensions to gray level images, hit or miss transformation, basic morphologic algorithms.

Module 3:

Format-Based Forensics- Fourier Transform-Smoothing and Sharpening, frequency domain filters- Ideal, Butterworth and Gaussian Filters, Homomorphic filtering, JPEG, Camera-Based Forensics. Pixel-Based Forensics: Resampling, Cloning, Thumbnails.

Module 4:

Principal Component Analysis, Linear Discriminant Analysis, Quadratic Discriminant Analysis and Logistic Regression, Computer Generated or Photographic: Perception.

Module 5:

Motion, Re-Projected,Projectile,Enhancement Physics-BasedForensics:2-DLighting,LeeHarvey Oswald (case study). Image Hiding, Image Coding. Image file Forensics, Video Surveillance, RFID and Vehicular tracking (GPS) devices, Image security techniques: visual cryptography, Stenography, water marking.

Labs / Practicals:

NA

References:

1. N.Efford,DigitalImageProcessing,AddisonWesley2000,ISBN0-201-59623-7
2. M Sonka, VHlavac and RBoyle, Image Processing, Analysis and Machine Vision, PWS 1999,ISBN0-534-95393
3. Pratt.W.K., Digital Image Processing, JohnWileyandSons,NewYork,1978

Course Code	Course Name	L	T	P	Cr
DCSA250035	Information Security Audit	3	0	2	4

Course Outcomes:

CO1: Discussed various algorithms and Distributions.
CO2: Understanding the approaches of message authentication
CO3: Analyze the security principles and its requirements
CO4: Apply the roles and procedures for audit
CO5: Analyze the approaches to audits during the system development

Module 1:

A model for Internetwork security, Conventional Encryption Principles & Algorithms (DES, AES, RC4, Blowfish), Block Cipher Modes of Operation, Location of Encryption Devices, Key Distribution. Public key cryptography principles, public key cryptography algorithms (RSA, Diffie- Hellman, ECC), public Key Distribution.

Module 2:

Approaches of Message Authentication - Secure Hash Functions (SHA-512, MD5) and HMAC, Digital Signatures, Kerberos, X.509 Directory Authentication Service, Email Security: Pretty Good Privacy (PGP) IP Security: Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management.

Module 3:

Web Security: Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET). Firewalls: Firewall Design principles, Trusted Systems, Intrusion Detection Systems.

Module 4:

Auditing For Security: Introduction, Basic Terms Related to Audits, Security audits, The Need for Security Audits in Organization, Organizational Roles and Responsibilities for Security Audit, Auditors Responsibility In Security Audits, Types Of Security Audits.

Module 5:

Information Security Assessments: Vulnerability Assessment, Classification, Types of Vulnerability Assessment, Vulnerability Assessment Phases, Vulnerability Analysis Stages, Characteristics of a Good Vulnerability Assessment Solutions &Considerations, Vulnerability Assessment Reports – Tools and choosing a right Tool, Information Security Risk Assessment, Risk Treatment, Residual Risk, Risk Acceptance, Risk Management Feedback Loops etc.

Labs / Practicals:

NA

References:

1. Information Security by Mark Stamp, Wiley–INDIA, 2006.
2. Fundamentals of Computer Security, Springer.
3. Network Security: The complete reference, Robert Bragg, Mark Rhodes, TMH
4. Computer Security Basics by Rick Lehtinen, Deborah Russell & G. T. Gangemi Sr., SPD O"REILLY 2006.
5. Modern Cryptography by Wenbo Mao, Pearson Education2007.
6. Principles of Information Security, Whitman, Thomson.

Course Code	Course Name	L	T	P	Cr
DCSE250023	Cloud Computing Security	3	1	0	4

Course Outcomes:

CO1:Understand the fundamental principles of cloud computing.
CO2:Remember the importance of virtualization in distributed computing and how this has enabled the development of Cloud Computing.
CO3:Analyze the performance of Cloud Computing.
CO4:Apply the Concept of Cloud Infrastructure Model.
CO5:Analyze the concept of Cloud Security.

Module 1:

Cloud Computing Essentials, Overview of Cloud Computing, Cloud Security Baselines, Cloud Security, Privacy, and Trust Baselines, Infrastructure as a Service (IaaS)

Module 2:

Risk and Trust Assessment: Schemes for Cloud Services, Managing Risk in the Cloud, Cloud Security Risk Management, Secure Cloud Risk Management: Risk Mitigation Methods, Specification and Enforcement of Access Policies in Emerging Scenarios, Cryptographic Key Management for Data Protection, Cloud Security Access Control: Distributed Access Control, Cloud Security Key Management: Cloud User Controls, Cloud Computing Security Essentials and Architecture, Cloud Computing Architecture and Security Concepts, Secure Cloud Architecture.

Module 3:

Locking Down Cloud Servers, Third-Party Providers Integrity Assurance for Data Outsourcing, Negotiating Cloud Security Requirements with Vendors, Managing Legal Compliance Risk in the Cloud and Negotiating Personal Data Protection Requirements with Vendors, Integrity Assurance for Data Outsourcing, Secure Computation outsourcing

Module 4:

Computation Over Encrypted Data, Trusted Computing Technology, Computing
Technology for Trusted Cloud Security, Trusted Computing Technology and
Proposals for Resolving Cloud Computing Security Problems, Assuring Compliance with Government Certification and Accreditation Regulations, Government Certification, Accreditation, Regulations, and Compliance Risks, Simplifying Secure Cloud Computing Environments with Cloud Data Center, Availability, Recovery, and Auditing across Data Centers

Module 5:

Advanced Security Architectures for Cloud Computing, Side-Channel Attacks and Defenses on Cloud Traffic, Clouds Are Evil, Future Directions in Cloud Computing Security: Risks and Challenges

Labs / Practicals:

NA

References:

1. Krutz, Ronald L., and Russell Dean Vines. Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing, 2010.
2. Carlin, Sean, and Kevin Curran. "Cloud computing security." Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments. IGI Global, 2013. 12-17.

Course Code	Course Name	L	T	P	Cr
DCSE250049	Data Privacy	3	0	2	4

Course Outcomes:

CO1: To introduce the fundamentals of statistics, data privacy & polices.
CO2: To Study the mathematical model and computing practices
CO3: To learn the protection models and surveys
CO4: To study the computation system
CO5: Aware of policies and practices of technology

Module 1:

Data Privacy and its Importance- Need for Sharing Data, Methods of Protecting Data, Importance of Balancing Data Privacy and Utility, Disclosure, Tabular Data, Micro data, Approaches to Statistical disclosure control, Ethics, principles, guidelines and regulations.

Module 2:

Micro data-Disclosure, Disclosure risk, Estimating re-identification risk, Non-perturbative micro data masking, Perturbative micro data masking, Information loss in micro data.

Module 3:

Static Data Anonymization on Multidimensional Data -Privacy Preserving Methods, Classification of Data in a Multidimensional Data Set, Group- Based Anonymization, k-Anonymity, l-Diversity, t-closeness.

Module 4:

Static Data Anonymization on Complex Data Structures -Privacy Preserving Graph Data, Privacy Preserving Time Series Data, Time Series Data Protection Methods, Privacy Preservation of Longitudinal Data, Privacy Preservation of Trans- action Data.

Module 5:

Data Anonymization Threats-Threats to Anonymized Data, Threats to Data Structures, Threats by Anonymization Techniques, Randomization, k- Anonymization, l-Diversity, tCloseness. Dynamic Data Protection: Tokenization, Understanding Tokenization, Use Cases for Dynamic Data Protection, Benefits of Tokenization Compared to Other Methods, Components for Tokenization.

Labs / Practicals:

NA

References:

1. George T. Duncan. Mark Elliot, Juan-Jose Salazar-GonZalez, Statistical Confidentiality: Principle and Practice. Springer, 2011. (ISBN No.: 978-1-44-197801-1).
2. Aggarwal, Charu C., Yu, Philip S., Privacy-Preserving Data Mining: Models and Algorithms, Springer, 2010. (ISBN No.: 978-0-38-770991-8). Mode of Evaluation: CAT / Assignment / Quiz / FAT / Project / Seminar

Course Code	Course Name	L	T	P	Cr
DCSE250072	Edge Computing	3	1	0	4

Course Outcomes:

CO1: This course will explore research, frameworks, and applications in Edge Computing
CO2: The class will begin with are view of current IoT Applications
CO3: Explore frameworks for computing using Raspberry Pi
CO4: Apply the Interfacing edge to cloud applications
CO5: Analyze edge computing with others

Module 1:

IntroductiontoEdgeComputingScenario'sandUsecases-Edgecomputingpurposeanddefinition, Edge computing use cases, Edge computing hardware architectures, Edge platforms, Edge vs Fog Computing, Communication Models - Edge, Fog and M2M.

Module 2:

A connected ecosystem, IoT versus machine-to-machine versus, SCADA, The value of a network and Metcalfe's and Beckstrom's laws, IoT and edge architecture, Role of an architect, Understanding Implementations with examples-Example use case and deployment.

Module 3:

Introduction to Raspberry Pi, About the Raspberry Pi Board: Hardware Layout and Pinouts, Operating Systems on Raspberry Pi, Configuring Raspberry Pi, Programming Raspberry Pi, Connecting Raspberry Pi via SSH, Remote access tools, Interfacing DHT Sensor with Pi, Pi as Web server, Pi Camera, Image & Video Processing using Pi.

Module 4:

Implementation of Microcomputer Raspberry Pi and device Interfacing, Edge to Cloud Protocols, MQTT, MQTT publish-subscribe, MQTT architecture details, MQTT state transitions, MQTT packet structure, MQTT data types, MQTT communication formats, MQTT3.1.1working example.

Module 5:

Edge computing with Raspberry Pi, Industrial and Commercial IoT and Edge, Edge computing and solutions, Case study – Telemedicine palliative care, Requirements, Implementation, Use case retrospective.

Labs / Practicals:

NA

References:

1. Fog and Edge Computing: Principles and Paradigms by Rajkumar Buyya, SatishNarayanaSrirama, wiley publication, 2019, ISBN: 9781119524984.
2. David Jensen, “Beginning Azure IoT Edge Computing: Extending the Cloud to the Intelligent Edge, MICROSOFT AZURE

Course Code	Course Name	L	T	P	Cr
DCSE250073	Ethical Hacking	2	1	2	4

Course Outcomes:

CO1: Explain the ethical hacking process and distinguish between various attack vectors, hacker types, and phases of penetration testing.
CO2: Apply reconnaissance techniques such as footprinting, scanning, and enumeration to gather information about target systems.
CO3: Demonstrate the ability to exploit system and network vulnerabilities using tools and techniques like password cracking, sniffing, and privilege escalation.
CO4: Identify and exploit web application and wireless network vulnerabilities using ethical hacking tools and analyze the associated risks.
CO5: Prepare and document penetration testing reports while adhering to legal and ethical standards of cybersecurity practice.

Module 1:

Ethical Hacking Process & Reconnaissance: Ethical hacking methodology
Hacker mindset, anonymity, legality, ethics, Information gathering, techniques (active & passive), Physical security weaknesses, Internal & external testing, Penetration test planning and reporting

Module 2:

Social Engineering & Password Attacks: Types of social engineering, Phishing, pretexting, tailgating, Password cracking techniques (brute force, dictionary), Privilege escalation, Countermeasures

Module 3:

Sniffing & Network Scanning: Packet sniffing methods, ARP spoofing, DNS/IP sniffing, Network scanning tools and techniques

Module 4:

System and Wireless Hacking: System hacking: vulnerability discovery, keystroke logging, remote exploits, Wireless hacking: WEP/WPA weakness, wireless traffic capturing, cracking

Module 5:

Web & Application Hacking: Web-based attacks: SQL Injection, XSS, file inclusion, Use of tools like Nikto, Burp Suite, Metasploit, Wireless, Web app vulnerability exploitation and reporting

Labs / Practicals:

1. Experiment No.1: Footprinting and Reconnaissance: Perform passive and active information gathering on a target website or IP using tools like whois, nslookup, the Harvester, and Recon-ng.
2. Experiment No.2: Scanning Networks: Use Nmap or Zenmap to discover open ports, services, and operating systems on a target machine.
3. Experiment No.3: Enumeration: Enumerate usernames, shared resources, and services using tools like NetBIOS, SNMPwalk, or enum4linux.
4. Experiment No.4: System Hacking – Password Cracking: Perform password cracking using tools like John the Ripper, Hydra, or Hashcat.
5. Experiment No.5: Malware Analysis (Static and Dynamic): Analyze a sample malware in a sandbox environment using tools like PEStudio, Process Monitor, or Wireshark.
6. Experiment No.6: Sniffing and Spoofing: Capture and analyze network packets using Wireshark or tcpdump; perform ARP spoofing using Ettercap or Cain and Abel.
7. Experiment No.7: Session Hijacking: Demonstrate session hijacking using tools like Ettercap or browser

cookie stealing techniques in a controlled environment.
8. Experiment No.8: Denial of Service (DoS) Attack: Simulate a DoS attack using tools like Hping3, LOIC, or custom scripts to understand impact and prevention.
9. Experiment No.9: Web Server Footprinting and Vulnerability Scanning: Perform vulnerability scanning on a web server using tools like Nikto, OpenVAS, or Nessus.
10. Experiment No.10: SQL Injection Attack: Demonstrate SQL injection on a test web application using tools like sqlmap or manual techniques.
11. Experiment No11: Cross-Site Scripting (XSS) Attack: Perform stored and reflected XSS attacks on a vulnerable web application like DVWA (Damn Vulnerable Web Application).
12. Experiment No.12: Cross-Site Request Forgery (CSRF) Attack: Simulate CSRF attacks using web applications like DVWA or custom scripts to understand defense mechanisms.
13. Experiment No.13: Privilege Escalation: Perform privilege escalation in a Linux or Windows environment using local exploits or misconfigurations.
14. Experiment No.14: Wireless Hacking: Crack WPA/WPA2 passwords using aircrack-ng suite and perform wireless network analysis.
15. Experiment No.15: Creating a Penetration Testing Report: Conduct a full penetration test on a test system or network and document findings, tools used, vulnerabilities, and mitigation strategies.

References:

1. Harris, S., Harper, A., Eagle, C., & Ness, J. (Year). Gray Hat Hacking: The Ethical Hacker’s Handbook. TMH.
2. Erickson, J. (Year). Hacking: The Art of Exploitation. SPD.
3. Beaver, K. (2013). Hacking for Dummies (3rd ed.). Wiley.
4. Additional: Shon Harris et al., Gray Hat Hacking (TMH); Thomas Mathew, Ethical Hacking (OSB).

Course Code	Course Name	L	T	P	Cr
DCSE250075	Forensic Psychology	3	1	0	4

Course Outcomes:

CO1:Understanding the psychology of historical roots
CO2:To know about the structure of biology and its behaviours
CO3:Identify the concepts of Psychologists and investigation
CO4:To assess the Risks involved in Forensics Psycology.
CO5:Understanding the various Interrogations and Confessiona

Module 1:

The history of psychology, issues of psychology,modern perspectives, the scientific methodology, issues in psychology, ethics of psychological research. The biological perspective: Neurons and nerves, an overview of the nervous system, distant connection, looking inside living brain, from the bottom up. Sensation and perception: The ABCs of sensation, the science of seeing, the hearing sense, chemical sense somesthetics sense, The ABCs perception.
Conciousness : sleep, dreams effects of hypnosis, influence of psychoactive drugs.

Module 2:

Classical conditioning, operant conditioning, cognitive leaning theory,
observational learning. Memory: three memory system, retrieval of long term memories, reconstructive nature of long term memory retrival, neuroscience of memory, health and memory

Module 3:

Forensic psychology, forensic psychologists, psychology and law enforcement, techniques of criminal investigation

Module 4:

Insanity and competency, From dangerousness to risk assessment, Syndrome evidence, child sexual abuse, child custody and related decisions, improving eyewitness identification procedures.

Module 5:

Performance Metrics- General issues- Partitioning the patterns for training, testing,and validation-Cross validation - Fitness and fitness functions - Parametric and nonparametric statistics, Evolutionary algorithm effectiveness metrics, Receiver operating characteristic curves, Computational intelligence tools for explanation facilities, Case Studies for implementation of practical applications in computational intelligence.

Labs / Practicals:

NA

References:

1. Psychology, by Saundra K. Ciccarelli Gulf Coast State College J. Noland White Georgia College 4th edition. (unit 1 &2)
2. Forensic Psychology, by Solomon M.Fulero & Lawrence S. Wrightsman 3rd edition. (unit 3,4,5)

Course Code	Course Name	L	T	P	Cr
DCSE250104	Operating Systems Security	3	0	2	4

Course Outcomes:

CO1:Understand and analyze operating systems Security
CO2:Analyze Security Kernels
CO3:Apply the concept of commercial OS
CO4:Analyze secure Virtual Machine Systems
CO5:Apply the functionalities in Solaris

Module 1:

Secure Operarting Systems-Security Goals-Trust Model- Threat Model. Access Control Fundamentals-Protection System-Reference MonitorSecure Operating Definition.Multics- Multics System-Multics Security- Multics Vulnerability Analysis

Module 2:

Security in OS & Goals System Histories-UNIX Security- Windows SecurityInformation Flow- Information Flow Secrecy Models, Information flow integrity
models- Covert Channels.

Module 3:

Security Kernels & Securing Commercial OS Secure Communications ProcessorArchitecture, Hardware, Trusted Operating Program, Kernel Interface Package,
Applications, Gemini Secure Operating System-Retrofitting Security into a Commercial OS- History of Retrofitting Commercial OS-Commercial EraMicrokernel Era- Unix Era

Module 4:

Secure Virtual Machine Systems Separation Kernels-VAX VMM Security KernelVAX VMM Design - VAX VMM Evaluation - VAX VMM Result- Security in other virtual Machine Systems- System Assurance

Module 5:

Solaris Trusted Extensions-Trusted Extensions Access ControlSolaris Compatibility-Trusted Extensions Mediation-Process Rights
Management-Role Based Access Control – Trusted Extensions Networking Multilevel Services-Administration-Linux Security Modules-Security Enhanced
Linux.

Labs / Practicals:

NA

References:

1. Mukesh Singhal, Niranjan G Shivratri , “Advanced Concepts in Operating Systems”, McGraw Hill International, 1994.
2. Pradeep Kumar Sinha, “Distributed Operating Systems: Concepts and Design“, PHI, 2002.

Course Code	Course Name	L	T	P	Cr
DCSE250125	Web and Database Security	3	1	0	4

Course Outcomes:

CO1:Identify common application vulnerabilities
CO2:Analyze the concepts of quantum cryptography
CO3:Analyze the Web architecture and applications
CO4:Examine, how common mistakes can be bypassed and exploit the application
CO5:Apply client side and service side programming

Module 1:

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

Module 2:

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

Module 3:

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

Module 4:

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

Module 5:

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

Labs / Practicals:

Preparing

References:

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

Course Code	Course Name	L	T	P	Cr
DOAI250017	Data Analytics for Fraud Detection	3	0	2	4

Course Outcomes:

CO1: Understand various types of fraud, their characteristics, and the role of data analytics in fraud detection.
CO2:Apply data preprocessing and exploratory data analysis techniques on real-world fraud datasets.
CO3:Build and evaluate machine learning models for detecting fraudulent activities.
CO4:Implement unsupervised and real-time fraud detection techniques using big data tools.
CO5:Analyze ethical, legal, and privacy considerations in fraud analytics and present practical fraud detection solutions.

Module 1:

Introduction to Fraud and Data Analytics :
What is Fraud? Types of Fraud (Financial, Identity Theft, Insurance, Healthcare, Cyber Fraud, etc.), Fraud Triangle Theory and Red Flags, Importance and Role of Data Analytics in Fraud Detection, Overview of the Fraud Detection Lifecycle, Data Analytics Workflow in Fraud Detection, Case Studies: Enron, Wells Fargo, etc.

Module 2:

Data Preprocessing and Exploration for Fraud Analytics :
Data Collection Methods and Challenges, Data Cleaning and Normalization Techniques, Handling Imbalanced Data (Oversampling, SMOTE, Undersampling), Feature Engineering: Domain-Specific Feature Creation, Exploratory Data Analysis (EDA): Detecting Anomalies and Patterns, Visualization Techniques for Fraud Trends

Module 3:

Machine Learning Techniques for Fraud Detection :
Supervised Learning Methods: Logistic Regression, Decision Trees, Random Forest, XGBoost, Unsupervised Learning: Clustering, Isolation Forest, Autoencoders, One-Class SVM, Evaluation Metrics: Precision, Recall, F1-Score, ROC-AUC, Model Validation and Cross-Validation Techniques, Model Interpretability: SHAP, LIME

Module 4:

Real-Time and Advanced Fraud Detection Systems :
Introduction to Streaming Data and Real-Time Fraud Detection, Anomaly Detection in Streaming Data using Spark, Kafka, Rule-based vs AI/ML-based Detection Systems, Big Data Platforms for Fraud Analytics: Hadoop, Spark, Introduction to Graph-Based Fraud Detection (Social Networks, Transaction Networks)

Module 5:

Ethics, Case Studies, and Industry Applications :
Ethics in Fraud Analytics: Privacy, Fairness, Bias, Legal Aspects and Compliance (AML, GDPR, PCI-DSS), Fraud Detection in Banking, Insurance, Healthcare, E-Commerce, Recent Trends: AI in Fraud Detection, Blockchain Use

Labs / Practicals:

1. Perform EDA on a credit card fraud dataset to identify trends and anomalies.
2. Clean and preprocess transactional data by handling missing values and normalization.
3. Apply SMOTE or undersampling to balance an imbalanced fraud detection dataset.
4. Build and evaluate a logistic regression model for fraud classification.
5. Compare Decision Tree and Random Forest models on fraud detection accuracy.
6. Implement Isolation Forest or KMeans for unsupervised fraud detection.
7. Simulate real-time fraud alerts using Kafka and Spark streaming.
8. Use SHAP or LIME to interpret a fraud detection model's predictions.
9. Model transaction data as a graph and detect fraud rings using NetworkX.
10. Create an end-to-end fraud detection project from data cleaning to model deployment.

References:

1. "Fraud Analytics: Strategies and Methods for Detection and Prevention" – Bart Baesens
2. "Data Science for Business" – Foster Provost and Tom Fawcett
3. "Practical Fraud Prevention" – Gilit Saporta
4. Research papers, white papers, and industry reports from SAS, KPMG, and Deloitte

Course Code	Course Name	L	T	P	Cr
DOEE250124	IOT and its Applications	3	1	0	4

Course Outcomes:

CO1: Understand the basics of IoT.
CO2: Implement the state of the Architecture of an IoT.
CO3: Understand design methodology and hardware platforms involved in IoT.
CO4: Understand how to analyze and organize the data.
CO5: Compare IOT Applications in Industrial & realworld.

Module 1:

FUNDAMENTALS OF IoT- Evolution of Internet of Things, Enabling Technologies, M2M Communication, IoT World Forum (IoTWF) standardized architecture, Simplified IoT Architecture, Core IoT Functional Stack, Fog, Edge and Cloud in IoT, Functional blocks of an IoT ecosystem, Sensors, Actuators, Smart Objects and Connecting Smart Objects.

Module 2:

IoT PROTOCOLS- IoT Access Technologies: Physical and MAC layers, topology and Security of IEEE 802.15.4, 802.11ah and Lora WAN, Network Layer: IP versions, Constrained Nodes and Constrained Networks,6LoWPAN, Application Transport Methods: SCADA, Application Layer Protocols: CoAP and MQTT.

Module 3:

DESIGN AND DEVELOPMENT- Design Methodology, Embedded computing logic, Microcontroller, System on Chips, IoT system building blocks
IoT Platform overview: Overview of IoT supported Hardware platforms such as: Raspberry pi, Arduino Board details

Module 4:

DATA ANALYTICS AND SUPPORTING SERVICES:
Data Analytics: Introduction, Structured Versus Unstructured Data, Data in Motion versus Data at Rest, IoT Data Analytics Challenges, Data Acquiring, Organizing in IoT/M2M,
Supporting Services: Computing Using a Cloud Platform for IoT/M2M Applications/Services, Everything as a service and Cloud Service Models.

Module 5:

CASE STUDIES/INDUSTRIAL APPLICATIONS: IoT applications in home, infrastructures, buildings, security, Industries, Home appliances, other IoT electronic equipments, Industry 4.0 concepts.

Labs / Practicals:

NA

References:

1. The Internet of Things – Key applications and Protocols, Olivier Hersent, David Boswarthick, Omar Elloumi and Wiley, 2012 (for Unit2).
2. “From Machine-to-Machine to the Internet of Things – Introduction to a New Age of Intelligence”,Jan Ho¨ ller, VlasiosTsiatsis, Catherine Mulligan, Stamatis,

Karnouskos, Stefan Avesand. David Boyle and Elsevier, 2014.
3. Architecting the Internet of Things,Dieter Uckelmann, Mark Harrison, Michahelles and Florian (Eds), Springer,2011.
4. Recipes to Begin, Expand, and Enhance Your Projects, 2nd Edition,Michael Margolis,Arduino Cookbook and O"Reilly Media,2011.