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

(2025-26 Scheme)

रा.इ.सू.प्रौ.सं

NIELIT

Deemed to be University

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

Vision

To be a premier center of excellence in Cyber Forensics education, research, and innovation, fostering globally competent professionals who safeguard digital ecosystems through cutting-edge forensic techniques, ethical practices, and technological leadership.

Mission

The mission of the M.Tech in Cyber Forensics program is to equip students with advanced knowledge and practical expertise in digital forensics, cybersecurity, and investigative methodologies. The program aims to foster analytical thinking, innovation, and ethical responsibility to prepare graduates for critical roles in securing digital assets, conducting cyber investigations, and contributing to national and global cybersecurity efforts.

Program Education Objectives

PEO1: Attain in-depth expertise in cyber forensics, digital investigation, and cybersecurity, grounded in strong theoretical and practical foundations.
PEO2: Excel in careers in law enforcement, intelligence, private sector cybersecurity, and academic research by addressing complex cybercrime and digital evidence challenges.
PEO3: Demonstrate leadership, collaboration, and communication skills while contributing to technological advancements and policy formulation in cyber law and digital security.
PEO4: Adapt to emerging trends, legal frameworks, and technologies in the evolving landscape of digital forensics, cybersecurity, and privacy protection.

Program Outcomes

PO1: Ability to independently conduct investigations and research in cyber forensics and digital crime analysis.
PO2: Ability to write, present, and publish substantial technical reports, forensic case documentation, and scholarly research in cyber forensics and cybersecurity domains.
PO3: Mastery of tools and techniques in cyber forensics, including evidence acquisition, digital artifact analysis, memory forensics, and malware analysis.
PO4: Proficiency in using forensic and cybersecurity tools such as EnCase, FTK, Autopsy, Wireshark, and Metasploit for practical case resolution.
PO5: Capacity for continuous learning, innovation, and ethical decision-making to handle emerging cyber threats, legal challenges, and privacy concerns.

Program Specific Outcomes

PSO1: Apply forensic methodologies to identify, preserve, analyze, and present digital evidence in alignment with legal and investigative standards.
PSO2: Design and implement secure systems and incident response strategies to detect and mitigate cyber threats in real-time.
PSO3: Analyze malware behavior, cyber attacks, and data breaches using automated tools and reverse engineering techniques.
PSO4: Demonstrate knowledge of cyber laws, digital ethics, and regulatory compliance in national and international contexts.
PSO5: Engage in advanced research and innovation in areas such as mobile forensics, IoT forensics, blockchain forensics, and AI-assisted threat intelligence.

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-MTECFS-101	DCSE250043	Cryptography and Network Security	3	0	2	4
PE-MTECFS-102	Elective	Program Elective				4
OE-MTECFS-103	Elective	Open Elective				4
PC-MTECFS-104	DASH250095	Research Methodology and IPR	3	1	0	4
AU-MTECFS-105	Elective	Audit Elective				0
PC-MTECFS-106	DCSE250065	Digital Forensics & Cyber Crime Investigation	3	0	2	4

Semester 2						
Semester Code	**Course Code**	**Course Title**	**L**	**T**	**P**	**Cr**
PC-MTECFS-201	DCSA250021	Cyber Law	3	1	0	4
PC-MTECFS-202	DCSE250092	Mobile & Digital Forensic	3	0	2	4
PE-MTECFS-203	Elective	Program Elective				4
PE-MTECFS-204	Elective	Program Elective				4
AU-MTECFS-205	Elective	Audit Elective				0
EE-MTECFS-206	EE	Mini Project				4

Semester 3						
Semester Code	**Course Code**	**Course Title**	**L**	**T**	**P**	**Cr**
PE-MTECFS-301	Elective	Program Elective				4
OE-MTECFS-302	Elective	Open Elective				4
EE-MTECFS-303	EE	Dissertation-I /Internal Project				12

Semester 4						
Semester Code	**Course Code**	**Course Title**	**L**	**T**	**P**	**Cr**
EE-MTECFS-401	EE	Dissertation-II				20

Elective Courses

Elective Courses for PE Category						
Course Code	**Course Title**	**L**	**T**	**P**	**Cr**	**For Sem./Code**
DCSE250019	Cloud Architecture and Security	3	0	2	4	102
DCSE250093	Mobile & Wireless Security	3	0	2	4	102
DOAI250017	Data Analytics for Fraud Detection	3	0	2	4	102
DCSA250035	Information Security Audit	3	0	2	4	103
DCSE250049	Data Privacy	3	0	2	4	103
DCSE250072	Edge Computing	3	1	0	4	103
DCSA250005	Applied Cryptography	3	1	0	4	203
DOAI250032	Machine Learning	3	0	2	4	203
DOEE250124	IOT and its Applications	3	1	0	4	203
DCSA250008	Biometrics	3	1	0	4	301
DCSA250009	Blockchain Technology	3	1	0	4	301
DCSA250033	Image Forensics and Security	3	0	2	4	301

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
DCSE250043	Cryptography and Network Security	3	0	2	4

Course Outcomes:

CO1: Explain security fundamentals, including the CIA Triad and various cyber threats.
CO2: Describe security services and mechanisms, such as authentication and encryption.
CO3: Understand the history and evolution of cryptography, including classical techniques.
CO4: Recognize the role of cryptanalysis in breaking cryptographic systems.
CO5: Apply mathematical foundations, including number theory, modular arithmetic, and random number generation, in cryptographic algorithms.

Module 1:

Introduction to Cryptography & Security Concepts
Basics of Security, Security Goals: Confidentiality, Integrity, Availability (CIA), Threats and Attacks: Passive vs. Active Attacks, Security Services & Mechanisms, Cybersecurity Principles, Introduction to Cryptography, History & Evolution of Cryptography, Classical Cryptographic Techniques: Caesar Cipher, Vigenère Cipher, Playfair Cipher, Modern Cryptography & Cryptanalysis
Mathematical Foundations of Cryptography: Number Theory Basics: Prime Numbers, Modular Arithmetic, Euler's Theorem, Greatest Common Divisor (GCD), Fermat's Theorem, Random Number Generation

Module 2:

Symmetric & Asymmetric Cryptography
Symmetric Key Cryptography, Block Ciphers vs. Stream Ciphers, Data Encryption Standard (DES) & Triple DES, Advanced Encryption Standard (AES), Modes of Operation: ECB, CBC, CFB, OFB, CTR, Asymmetric Key Cryptography, Public Key Cryptosystems: RSA Algorithm, Key Exchange Mechanisms: Diffie-Hellman Key Exchange, Elliptic Curve Cryptography (ECC), Comparison of Symmetric & Asymmetric Cryptography

Module 3:

Hash Functions, Digital Signatures & Authentication Cryptographic Hash Functions, Properties of Hash Functions, Common Hash Algorithms: MD5, SHA-1, SHA-256, SHA-3, Message Authentication, Message Authentication Codes (MAC), HMAC (Hash-based Message Authentication Code), Digital Signatures & Certificates, RSA Digital Signature Algorithm, Digital Certificates & Public Key Infrastructure (PKI), SSL/TLS Encryption and HTTPS Authentication Mechanisms, Password-Based Authentication, Multi-Factor Authentication (MFA), Biometric Authentication

Module 4:

Network Security & Secure Protocols
Network Security Fundamentals, Security in OSI & TCP/IP Models, Firewalls and Intrusion Detection Systems (IDS/IPS), Virtual Private Networks (VPNs) & IPsec, Secure Network Protocols, Secure Email: PGP & S/MIME, Secure Web Transactions: HTTPS, SSL/TLS
Wireless Security: WPA, WPA2, WPA3, Network Attacks & Defense Mechanisms, Denial of Service (DoS) & Distributed DoS (DDoS) Attacks, Man-in-the-Middle (MITM) & Eavesdropping, SQL Injection & Cross-Site Scripting (XSS)

Module 5:

Emerging Trends & Cybersecurity Applications

Blockchain & Cryptography, Role of Cryptography in Blockchain, Bitcoin & Ethereum Security, Cloud Security & Zero Trust Security Model, Cloud Encryption Mechanisms, Zero Trust Architecture & Access Control
Cybersecurity & Ethical Hacking, Introduction to Ethical Hacking, Penetration Testing Basics, Legal & Ethical Issues in Cybersecurity, Future Trends in Cryptography & Security

Labs / Practicals:

Preparing

References:

1. "The Joy of Cryptography" by Michael Rosulek
https://joyofcryptography.com/pdf/book.pdf

2. "Cryptography and Computer Security" by Chris Bourke
https://cse.unl.edu/~cbourke/cryptoNotes.pdf

3. "Applied Cryptography (20th Anniversary Edition)" by Bruce Schneier
https://www.schneier.com/books/applied-cryptography

4. "Cryptography and Network Security (Eighth Edition)" by William Stallings
http://williamstallings.com/Cryptography/Crypto8e-Student

5. "Cracking Codes With Python: An Introduction To Building And Breaking Ciphers" by Al Sweigart
https://inventwithpython.com/cracking

6. "Yet Another Introductory Number Theory Textbook (Cryptology Emphasis Version)" by Jonathan Adam Poritz
https://www.poritz.net/jonathan/share/yaintt.pdf

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
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
DCSE250092	Mobile & Digital Forensic	3	0	2	4

Course Outcomes:

CO1. Explain wireless technologies, identify security threats and vulnerabilities, and recommend protective measures against wireless and mobile attacks.
CO2. Analyze mobile communication security using the CIA triad and evaluate interception, codes, and SMS-related vulnerabilities in GSM systems.
CO3. Apply forensic techniques to extract, analyze, and preserve digital evidence from SIM cards, memory devices, and Android systems.
CO4. Demonstrate knowledge of digital forensics concepts, evidential potential of digital devices, and proper procedures for device handling and preservation.
CO5. Implement digital forensic examination principles, including imaging, hashing, audit logs, and evidence interpretation using structured security models.

Module 1:

Overview of wireless technologies and security: Personal Area Networks, Wireless Local Area Networks, Metropolitan Area Networks, Wide Area Networks. Wireless threats, vulnerabilities and security: Wireless LANs, War Driving, War Chalking, War Flying, Common Wi-Fi security recommendations, PDA Security, Cell Phones and Security, Wireless DoS attacks, GPS Jamming, Identity theft.

Module 2:

CIA triad in mobile phones-Voice, SMS and Identification data interception in GSM: Introduction, practical setup and tools, implementation- Software and Hardware Mobile phone tricks: Net monitor, GSM network service codes, mobile phone codes, catalog tricks and AT command set- SMS security issues.

Module 3:

Mobile phone forensics: crime and mobile phones, evidences, forensic procedures, files present in SIM card, device data, external memory dump, evidences in memory card, operators systems- Android forensics: Procedures for handling an android device, imaging android USB mass storage devices, logical and physical techniques.

Module 4:

Digital forensics: Introduction – Evidential potential of digital devices: closed vs. open systems, evaluating digital evidence potential- Device handling: seizure issues, device identification, networked devices and contamination.

Module 5:

Digital forensics examination principles: Previewing, imaging, continuity, hashing and evidence locations- Seven element security model- developmental model of digital systems- audit and logs- Evidence interpretation: Data content and context.

Labs / Practicals:

NA

References:

1. Gregory Kipper, “Wireless Crime and Forensic Investigation”, Auerbach Publications, 2007
2.IosifI.Androulidakis,“Mobilephonesecurityandforensics:Apractical approach”, Springer publications, 2012
3.AndrewHoog,“AndroidForensics:Investigation,AnalysisandMobileSecurity for Google Android”, Elsevier publications, 2011
4.AngusM.Marshall,“Digitalforensics:Digitalevidenceincriminalinvestigation”,John–WileyandSons,2008

Course Code	Course Name	L	T	P	Cr
DCSE250019	Cloud Architecture and Security	3	0	2	4

Course Outcomes:

CO1: Explain cloud models (Public, Private, Hybrid) and services (IaaS, PaaS, SaaS) with their benefits and challenges.
CO2: Describe cloud application deployment and compare platforms like AWS, Azure, and Google Cloud.
CO3: Apply basic cloud security concepts like authentication, access control, and data protection.
CO4: Identify virtualization and multi-tenancy issues, including VM isolation and recovery.
CO5: Outline cloud security management standards and data security practices across service models.

Module 1:

Computing Fundamental: Cloud computing definition, private, public and hybrid cloud. Cloud
aS, PaaS, SaaS. Benefits and challenges of cloud computing, public vs private clouds, role of
ation in enabling the cloud; Business Agility: Benefits and challenges to Cloud architecture.

Module 2:

Cloud Applications: Technologies and the processes required when deploying web
services-Deploying a web service from inside and outside a cloud architecture,
advantages and disadvantages- Development environments for service development;
Amazon, Azure, Google App.

Module 3:

Security Concepts: Confidentiality, privacy, integrity, authentication, nonrepudiation, availability, access control, defence in depth, least privilege- how these
concepts apply in the
cloud and their importance in PaaS, IaaS and SaaS. e.g. User authentication in the
cloud.

Module 4:

Multi-tenancy Issues: Isolation of users/VMs from each other- How the cloud
provider can provide this- Virtualization System Security Issues: e.g. ESX
and ESXi Security, ESX file system security- storage considerations, backup
and recovery- Virtualization System Vulnerabilities.

Module 5:

Management in the cloud – security management standards- SaaS, PaaS, IaaS
availability ent- access control- Data security and storage in cloud
and recovery- Virtualization System Vulnerabilities

Labs / Practicals:

NA

References:

1. GautamShroff,Enterprise Cloud Computing Technology Architecture Applications [ISBN: 978-0521137355]
2. Toby Velte, Anthony Velte, Robert Elsenpeter, Cloud Computing, A Practical Approach [ISBN: 0071626948]
3. Tim Mather, SubraKumaraswamy, ShahedLatif, Cloud Security and Privacy: An Enterprise Perspective on Risks and
Compliance [ISBN: 0596802765]
4. Ronald L. Krutz, Russell Dean Vines, Cloud Security [ISBN: 0470589876]

Course Code	Course Name	L	T	P	Cr
DCSE250093	Mobile & Wireless Security	3	0	2	4

Course Outcomes:

CO1: Describe wireless technologies and their security vulnerabilities.
CO2: Identify mobile network threats and attack types.
CO3: Explain physical layer security techniques in wireless systems.
CO4: Analyze security challenges in ad hoc wireless networks.
CO5: Evaluate RFID security and privacy protection methods.

Module 1:

WIRELESS NETWORK SECURITY THREATS AND VULNERABILITIES
Introduction to wireless technologies, Design Factors, security threats and vulnerabilities present at the different protocol layers, family of security protocols and algorithms used in the existing wireless networks (Bluetooth, Wi-Fi, Wi MAX and LTE standards).

Module 2:

Introduction To Mobile Network Techs, Vulnerabilities Threats And Attack Entry Points. Categorization Of Attacks In Mobile Networks, Signaling Attacks. Threats And Attacks In 4g Networks- Attacks Against Security And Confidentiality, Ip-Based Attacks, Gtp-Based Attacks, Volte Sip-Based Attacks, Diameter-Based Attacks.

Module 3:

Emerging physical layer security in wireless communications. Class of informationTheoretic security, artificial-noise-aided security, security-oriented beam forming,
security- oriented diversity, and physical-layer secret key generation techniques. Review on various wireless jammers, open challenges in wireless security.

Module 4:

Security in Ad Hoc Wireless Networks, Network Security Requirements, Issues and Challenges in Security Provisioning, Network Security Attacks, Key Management in Adhoc Wireless Networks, Secure Routing in Adhoc Wireless Networks.

Module 5:

Introduction, RFID Security and privacy, RFID chips Techniques and Protocols, RFID anti- counterfeiting, Man-in-the-middle attacks on RFID systems, Digital Signature Transponder, Combining Physics and Cryptography to Enhance Privacy in RFID Systems, Scalability Issues in Large-Scale Applications, An Efficient and Secure RFID Security Method with Ownership Transfer, Policy-based Dynamic Privacy Protection Framework leveraging Globally Mobile RFIDs, User-Centric Security for RFID based Distributed Systems, Optimizing RFID protocols for Low Information Leakage, RFID: an anti-counterfeiting tool.

Labs / Practicals:

NA

References:

1. Kia Makki, Peter Reiher, “Mobile and Wireless Network Security and Privacy “, Springer, ISBN 978-0-387-71057-0, 2007.
2. Siva Ram Murthy.C, Manoj B.S, “Adhoc Wireless Networks Architectures and By Yulong Zou, Senior Member IEEE, Jia Zhu, Xianbin Wang, Senior Member IEEE, and Lajos Hanzo, Fellow IEEE
3. “A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends” Zou et al.:

A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends
4. Noureddine Boudriga, ”Security of Mobile Communications”,
5. ISBN 9780849379413, 2010.
6. Kitsos, Paris; Zhang, Yan, “RFID Security Techniques, Protocols and System-On-Chip Design”, ISBN 978-0-387-76481-8, 2008.
7. Johny Cache, Joshua Wright and Vincent Liu,” Hacking Wireless Exposed: Wireless Security Secrets & Solutions “, second edition, McGraw Hill, ISBN: 978-0-07-166662-6, 2010.

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
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
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
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
DOAI250032	Machine Learning	3	0	2	4

Course Outcomes:

CO1: Identify and extract relevant features from raw IoT data suitable for applying appropriate Machine Learning (ML) techniques.
CO2: Evaluate and compare the strengths and limitations of various ML algorithms across diverse application domains, particularly in IoT.
CO3: Select and implement appropriate ML models based on data characteristics and application requirements.
CO4: Mathematically formulate and analyze ML models and algorithms, including their underlying assumptions and performance metrics.
CO5: Design and validate machine learning-based solutions for real-world problems in IoT, demonstrating practical understanding and technical proficiency.

Module 1:

Module 1
Introduction: Introduction to Machine Learning: Introduction. Different types of learning, Hypothesis space and inductive bias, Evaluation. Training and test sets, cross validation, Concept of over fitting, under fitting, Bias and Variance.
Linear Regression: Introduction, Linear regression, Simple and Multiple Linear regression, Polynomial regression, evaluating regression fit.

Module 2:

Module 2
Decision tree learning: Introduction, Decision tree representation, appropriate problems for decision tree learning, the basic decision tree algorithm, hypothesis space search in decision tree learning, inductive bias in decision tree learning, issues in decision tree learning, Python exercise on Decision Tree.
Instance based Learning: K nearest neighbor, the Curse of Dimensionality, Feature Selection: forward search, backward search, univariate, multivariate feature selection approach, Feature reduction (Principal Component Analysis), Python exercise on KNN and PCA. Recommender System: Content based system, Collaborative filtering based.

Module 3:

Probability and Bayes Learning: Bayesian Learning, Naïve Bayes, Python exercise on Naïve Bayes, Logistic Regression.
Support Vector Machine: Introduction, the Dual formulation, Maximum margin with noise, nonlinear SVM and Kernel function, solution to dual problem.

Module 4:

Artificial Neural Networks: Introduction, Biological motivation, ANN representation, appropriate problem for ANN learning, Perceptron, multilayer networks and the back propagation algorithm.

Module 5:

Ensembles: Introduction, Bagging and boosting, Random forest, Discussion on some research papers.
Clustering: Introduction, K-mean clustering, agglomerative hierarchical clustering, Python exercise on k-mean clustering.

Labs / Practicals:

1 Write a Python program that imports a dataset of your choice, displays the first five rows, and prints the data type of the DataFrame as a whole. Then, generate and display the statistical summary (mean, median, standard deviation, etc.) for each column and provide complete information about the DataFrame.

2 Write a Python program to import (or create) a dataset with missing values, display the count of missing values per column, and handle them using both imputation and dropping methods. Then, compare the dataset before and after handling missing values, and display the final cleaned dataset.
3 Write a Python program to load (or create) a dataset, split it into training and testing sets, and standardize the features using StandardScaler from sklearn. preprocessing. Finally, display the dataset before and after standardization to observe the changes.
4 Write a Python program to load (or create) a dataset, separate it into predictor variables (X) and target variable (y), and then split the dataset into training and testing sets. Finally, print both the training and testing datasets.
5 Apply EM algorithm to cluster a set of data stored in a .CSV file. Use the same data set for clustering using k-Means algorithm. Compare the results of these two algorithms and comment on the quality of clustering. You can add Python ML library classes in the program.
6 Write a Python program to load (or create) a dataset with missing values, count missing values in each column, and handle them by replacing with NaN, the column mean, and the most frequent value. Finally, display the dataset before and after performing the replacements.
7 Write a Python program to load (or create) a dataset, split it into training and testing sets, and apply feature scaling to the data. Finally, display the dataset before and after scaling to observe the changes.
8 Write a program to implement k-Nearest Neighbour algorithm to classify the iris data set. Print both correct and wrong predictions. Python ML library classes can be used for this problem.
9 Implement the working principle of Artificial Neural Network with feed forward and feed backward principle.
10 Implement and demonstrate the working of SVM algorithm for classification.

References:

1. Kevin P. Murphy, “Machine Learning: A Probabilistic Perspective”, MIT Press, 2012.
2. C. M. Bishop. Pattern Recognition and Machine Learning. First Edition. Springer, 2006. (Second Indian Reprint, 2015).
3. Tom M. Mitchell, “Machine Learning”, McGraw-Hill, 2010
4. P. Flach. Machine Learning: The Art and Science of Algorithms that Make Sense of Data. First Edition, Cambridge University Press, 2012.

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.

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
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