Pandit Deendayal Energy University

School of Technology

Department of Computer Science and Engineering

Post Graduate Curriculum Handbook (Academic Year 2024-28)

M.Tech. (Cyber Security)
w. e. f. July, 2024.

Vision

"To contribute to the society by imparting transformative education and producing globally competent professionals having multidisciplinary skills and core values to do futuristic research & innovations."

Mission

- To accord high quality education in the continually evolving domain of Computer Engineering by offering state-of-the-art undergraduate, postgraduate, doctoral programmes.
- To address the problems of societal importance by contributing through the talent we nurture and research we do:
- To collaborate with industry and academia around the world to strengthen the education and multidisciplinary research ecosystem.
- To develop human talent to its fullest extent so that intellectually competent and imaginatively exceptional leaders can emerge in a range of computer professions.

Program Educational Objectives (PEOs)

PEO-1. Graduate will be successfully recognized as superiors for their problem solving capabilities and professional skills in the field of Cyber Security.
PEO-2. Graduate pursue higher studies or research career by acquiring in depth knowledge in cyber security and allied fields.

Program Outcomes (POs)

PO-1: An ability to independently carry out research /investigation and development work to solve practical problems.
PO-2: An ability to write and present a substantial technical report/document.
PO-3: Students should be able to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program.
PO-4: Design and Innovate computing systems addressing diverse needs in the domain of cyber security.
PO-5: Analyze the requirements of cyber security and design operational strategies and policies.
PO-6: Use cyber security solutions to analyze ethical, legal and social implications to solve real world problems.

Course Outline (M.Tech. - Cyber Security)

Semester 1

Subjects	Teaching Scheme	Total Credits
Mathematical Foundations of Cyber Security	3-1-0	4
Essentials of Cryptography	3-0-0	3
Essentials of Cryptography Laboratory	0-0-2	1
Cyber Laws and forensics	3-0-0	3
System and Network Security	3-0-0	3
System and Network Security Laboratory	0-0-2	1
Blockchain-based Cyber Security	3-0-0	3
Scientific Writing and Professional Ethics	2-0-0	2
Total Credits		**20**

Semester 2

Subjects	Teaching Scheme	Total Credits
Machine Learning for Cyber Security	3-0-0	3
Machine Learning for Cyber Security Laboratory	0-0-2	1
Department Elective I	3-0-0	3
Department Elective I Laboratory	0-0-2	1
Department Elective II	3-0-0	3
Department Elective III	3-0-0	3
Department Elective IV	3-0-0	3
Research Methodology	2-0-0	2
Seminar		1
Total Credits		**20**

Semester 3

Subjects	Teaching Scheme	Total Credits
Project Phase -I		13
Summer Internship/ IEP (6 Weeks)		1

Semester 4

Subjects	Teaching Scheme	Total Credits
Project Phase – II and Dissertation		16

List of Electives

Industry Track		**Program Elective**	**L**	**T**	**P**	**H**	**C**
	PE-1	Web Security and Penetration Testing	3	0	0	3	3
	PE-2	Web Security and Penetration Testing Laboratory	0	0	2	2	1
	PE-3	Cyber Physical System Security	3	0	0	3	3
	PE-4	Cyber Threat Intelligence	3	0	0	3	3
	PE-5	Social Network Security and Privacy	3	0	0	3	3
Research Track		**Program Elective**	**3**	**0**	**0**	**3**	**3**
	PE-1	Advanced Topics in Cryptography	3	0	0	3	3
	PE-2	Advanced Topics in Cryptography Laboratory	0	0	2	2	1
	PE-3	Data Authorization and Privacy Preservation	3	0	0	3	3
	PE-4	Security Protocols	3	0	0	3	3
	PE-5	Hardware Security	3	0	0	3	3

1st Semester

Course Code					Mathematical Foundations for Cyber Security					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	1	0	4	4	25	50	25	-	-	100

COURSE OBJECTIVES

- To provide fundamental concept of abstract algebra.
- To study basic concepts of group theory and binary operations.
- To study different operations on ECC.
- To study advanced number theory concepts.

Unit-1: Introduction Group theory - normal series, solvable groups, nilpotent groups; Ring theory - rings and modules, prime ideals, nil and Jacobson radicals	**10 Hrs.**
UNIT2: Abstract Algebra Finitely generated modules, exact sequences, tensor products, primary decomposition, Noetherian rings, Artin rings; Field theory - field extensions, automorphism groups, Galois theory.	**10Hrs.**
UNIT3: Elliptic Curve Cryptography Basics of Polynomial Expressions, GCD, Modular arithmetic, Prime numbers, Basics of discrete logarithms, Elliptic Curve Cryptography Operations, Scalar multiplication problem, Bilinear pairing system	**10Hrs.**
UNIT4: Number Theory Euclidean algorithm, Fermat's theorem, Euler's theorem, Chinese remainder theorem, Primality Testing algorithms, Shannon Theory, Perfect Secrecy, Semantic Security	**12Hrs.**
	42Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understand the concepts related to the basics of group theory.
CO2- Demonstrate knowledge and understanding of finite group.
CO3- Develop understanding of algebraic structure ring and field.
CO4- Analyze the operations on Elliptic Curve Cryptography structure.
CO5- Formulate techniques by cryptographic operations.
CO6- Design algebraic modeling for real time applications.

TEXT/REFERENCEBOOKS

1. D.S.DummitandR.M.Foote, "AbstractAlgebra",JohnWiley
2. MichaelArtin,"Algebra",PearsonEducation.
3. J.A.Gallian,"ContemporaryAbstractAlgebra",NarosaPublishingHouse.
4. I.N.Herstein,"TopicsinAlgebra",Wiley.
5. N.Jacobson,"BasicAlgebraI",HindustanPublishingCompany.
6. WilliamStallings,"Cryptography andNetworkSecurityPrinciplesandPractice",PearsonEducation.

RESEARCH PAPERS

1. "On linear codes with random multiplier vectors and the maximum trace dimension property", Journal of Mathematical Cryptology
2. "RIS-Jamming: Breaking Key Consistency in Channel Reciprocity-based Key Generation", IEEE Transactions on Information Forensics and Security
3. "Optimizing Rectangle and Boomerang Attacks: A Unified and Generic Framework for Key Recovery", Journal of Cryptology

Course Code					Essentials of Cryptography					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	-	-	100

COURSE OBJECTIVES

- Learn the Cryptography Primitives.
- Understand the mathematical concepts of cryptography.
- Learn the applications of cryptography for data security.
- Compare the security strength of various cryptographic algorithms.
- Comprehend the design principals for a cryptographic system.

UNIT 1:Introduction Introduction to Cryptography, Types of adversary models and attacks, Classical Cryptography: Affine Cipher, Stream Cipher, One time Pad, Pseudo Random Number generation	**10 Hrs.**
UNIT 2: Symmetric Key Cryptography Polynomial Arithmetic, DES, 3DES, AES, Blowfish, Cryptanalysis of Symmetric Encryption, Modes of Block Cipher Operations, Types of adversary models and attacks	**12 Hrs.**
UNIT 3: Public Key Cryptography System Cryptographic hash functions, SHA, Message authentication, Zero knowledge proofs, Digital signature,RSA, Diffie-Hellman Key Exchange, MITM attack	**12 Hrs.**
UNIT 4: Key Management and Distribution Kerberos, X.509 authentication service, PKI Public Key Cryptography standard (PKCS), Cryptographic Applications.	**8 Hrs.**
	42 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Differentiate the Symmetric and Asymmetric encryption techniques.

CO2- Understand the mathematics for building a cryptographic algorithm.

CO3- Evaluate the security strength of a cryptographic algorithm.

CO4- Apply the appropriate cryptographic scheme to withstand against a security attack.

CO5- Use Hashing techniques to create the message digest.

CO6- Develop the key management solutions to safeguard real world applications.

TEXT/REFERENCE BOOKS

1. William Stallings, "Cryptography and Network Security Principles and Practice", Pearson Education.
2. Wade Trappe, Lawrence Washington, “Introduction to Cryptography with Coding Theory”, Pearson Education
3. Bruce Schneier, “Applied Cryptography: Protocols, Algorithms, and Source Code in C”, Wiley Computer Publishing.
4. Wenbo Mao, “Modern Cryptography: Theory and Practice”, Prentice Hall.
5. Douglas Stinson, “Cryptography: Theory and Practice”, Taylor & Francis
6. Mark Shand, and Jean Vuillemin. "Fast implementations of RSA cryptography." In Proceedings of IEEE 11th Symposium on Computer Arithmetic, pp. 252-259. IEEE, 1993.
7. Joan Daemen, and Vincent Rijmen. "AES proposal: Rijndael." (1999).
8. B. Neuman, B. Clifford, and Theodore Ts'o. "Kerberos: An authentication service for computer networks." IEEE Communications magazine 32, no. 9 (1994): 33-38.

Course Code					Essentials of Cryptography Laboratory					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
0	0	2	1	2	-	-	-	50	50	100

COURSE OBJECTIVES

- Learn the practical aspects of cryptography.
- Get the difference between the classical and modern cryptographic techniques.
- Recognize the consequences of security vulnerabilities
- Compare the computational cost of various cryptographic primitives
- Learn the design concepts of modern cryptographic algorithms

LIST OF EXPERIMENT

1.	**Cipher text processing, block cipher and stream cipher:** Break a ciphertext generated using affine cipher by brute-force approach, Implement the OFB mode. Use AES as block cipher algorithm.
2.	**Symmetric key cryptography algorithms:** Algorithms and cryptanalysis
3.	**Public key symmetric algorithms:** RSA with all required algorithms (Extended Euclidean, Efficient/fast Power Exponentiation), implement CCA-2 attack on RSA, man-in-middle attack on Diffie-Hellman Key exchange.
4.	**Digital signature and encryption algorithm:** Elgamal Algorithm for Encryption, Elgamal Algorithm for Digital Signature
5.	**Modular elliptic curve:** Modular elliptic curve with following functions: (a) Finding Points, (b) Point addition, (c) Doubling Point, (d) Multiplication of scalar with point
6.	**Key management and distribution:** SHA-256 algorithm, your own designed pseudorandom number generation

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Learn the practical aspects of Classical Cryptographic techniques.
CO2- Implement the symmetric cryptographic techniques.
CO3- Compare the computational strength of symmetric and asymmetric encryption techniques.
CO4- Analyze the method to convert security vulnerability into attack on a system.
CO5- Demonstrate the usage of hash functions for creating digital signatures.
CO6- Design a new Cryptographic algorithm.

TEXT/REFERENCE BOOKS

1. William Stallings, "Cryptography and Network Security Principles and Practice", Pearson Education.
2. Wade Trappe, Lawrence Washington, “Introduction to Cryptography with Coding Theory”, Pearson Education
3. Bruce Schneier, “Applied Cryptography: Protocols, Algorithms, and Source Code in C”, Wiley Computer Publishing.
4. Wenbo Mao, “Modern Cryptography: Theory and Practice”, Prentice Hall.
5. Douglas Stinson, “Cryptography: Theory and Practice”, Taylor & Francis.
6. Mark Shand, and Jean Vuillemin. "Fast implementations of RSA cryptography." In Proceedings of IEEE 11th Symposium on Computer Arithmetic, pp. 252-259. IEEE, 1993.
7. Joan Daemen, and Vincent Rijmen. "AES proposal: Rijndael." (1999).
8. B. Neuman, B. Clifford, and Theodore Ts'o. "Kerberos: An authentication service for computer networks." IEEE Communications magazine 32, no. 9 (1994): 33-38.

Course Code					Cyber Law and Forensics					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	-	-	100

COURSE OBJECTIVES

- To understanding the difference between physical crime prosecution and cybercrime prosecution.
- To understand the need for the Information Technology Act and its amendments.
- To conduct a computer and/or network forensics investigation including digital evidence collection and evaluation and legal issues involved in network forensics.
- To mitigate technical issues in acquiring court-admissible chains of evidence using various forensic tools that reconstruct criminally liable actions at the physical and logical levels are also addressed.

UNIT 1: Introduction to Cyber Law Basic Terminologies of Law, Need for Cyber Law, Introduction to Cyber Crime, Types of Cyber Crimes, Digital Signature and Electronic Signature, Legal Recognition of Electronic Records, Regulation of Certifying Authorities	**10 Hrs.**
UNIT 2: IT – Act 2000 and Its Amendments IT Act 2000 and its Amendments (Act 2008, Act 2009, Act 2016), Offenses, Cyber Ethics, E-commerce and Laws in India, Intellectual Property Protection, Case studies of Cyber Crimes in India prosecuted under IT Act	**11 Hrs.**
UNIT 3: Fundamentals of Cyber Forensics What are Cyber Forensics, difference between digital forensics and computer forensics. Basics of forensics, Historical perspective, and evolution of cyber forensics, Evidence Handling and Chain of Custody, Data Acquisition methods, Processing Crime and Incident scenes.	**11 Hrs.**
UNIT 4: Cyber Crime Investigating Methods Forensic Footprints and Various File Systems, Working with Windows and CLI Systems, Current Computer Forensic Tools, investigating different digital devices, Handling Metadata, Report writing.	**10 Hrs.**
	42 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understand the basic laws associated with cybercrime.
CO2- Distinguish between cybercrime and the physical crimes assisting digital forensics.
CO3- Applying IT Acts and its amendments to the case study of real-world crimes.
CO4- Applying knowledge of cyber law principles in analysing crime.
CO5- Apply data acquisition methods and evidence handling procedures.
CO6- Analyse use of cyber laws and forensic methods with case studies.

TEXT/REFERENCE BOOKS

1. Vakul Sharma, “Information Technology Law and Practice: Law & Emerging Technology Cyber Law”, Universal Law Publishing.
2. David S. Wall, “Cybercrime: The Transformation of Crime in the Information Age”, Wiley Computer.
3. Anirudh Rastogi, “Cyber Law of Information Technology and Internet”, LexisNexis.

RESEARCH PAPER

1. P. Sharma, D. Doshi and M. M. Prajapati, "Cybercrime: Internal security threat," 2016 International Conference on ICT in Business Industry & Government (ICTBIG), Indore, India, 2016, pp. 1-4, doi: 10.1109/ICTBIG.2016.7892727.
2. Y. Baturin, "Computer Crimes, Computer Security and Computer Law: Phenomenon’s Dynamics Notes from the Russian Chair of Computer Law," 2017 International Workshop on Engineering Technologies and Computer Science (EnT), Moscow, Russia, 2017, pp. 3-7, doi: 10.1109/EnT.2017.23.

Course Code					System and Network Security					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	-	-	3	3	25	50	25	-	-	100

COURSE OBJECTIVES

- To understand the basics of system and network security
- To identify various system and network vulnerabilities
- To learn various mitigation and prevention techniques
- To secure a system and network with various tools

UNIT 1: Vulnerabilities and Exploits in System Software Introduction to Program Binaries, GDB tool, Buffer Overflow in the Stack, Return to LibC attack, Format String Vulnerabilities, Integer Exploits.	**12 Hrs.**
UNIT 2: Prevention and Mitigation Techniques W^X, Canaries, Address Space Layout Randomization (ASLR), Hardware and compiler mitigations Capability and sandboxing systems: SGX, Trust zone.	**12 Hrs.**
UNIT 3: Hardware Security Power Analysis Attacks, Side-channel attacks, Physically Unclonable Functions, Hardware Trojan.	**08 Hrs.**
UNIT 4: Network Security OSI and TCP Model Architecture, Public Networks Vulnerabilities, Network Security Protocols: SSL, Use of Packet Sniffer tool and Intrusion detection technique to detect the cyber attacks	**10 Hrs.**
	42 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Illustrate the concepts of system software and computer networks.

CO2- Understand the program binaries, debugging and analysis, buffer overflow vulnerabilities, string vulnerabilities and integer exploits.

CO3- Identify the vulnerabilities existing in a program code.

CO4- Apply the mitigation and prevention techniques existing in the system.

CO5- Analyze the vulnerabilities in public networks, potential impact and mitigation strategies.

CO6- Assess the security implications of power analysis attack, Side Channel Attack, Physically Unclonable Function, Trojan in hardware architecture.

TEXT/REFERENCE BOOKS

1. William Stallings, “Network Security Essentials: Applications and Standards”, Prentice Hall.
2. Michael T. Goodrich and Roberto Tamassia, “Introduction to Computer Security”, Addison Wesley.
3. W. Stallings, “Cryptography and Network Security: Principles and Practice”, Prentice Hall.
4. One, Aleph. "Smashing the stack for fun and profit." Phrack magazine.
5. B. Bierbaumer, K. Julian, K. Thomas, A.Francillon, and A. Zarras. "Smashing the stack protector for fun and profit." In ICT Systems Security and Privacy Protection: 33rd IFIP TC 11 International Conference, SEC 2018, Proceedings 33, pp. 293-306. Springer International Publishing, 2018.
6. D. Ahmad,. "The rising threat of vulnerabilities due to integer errors." IEEE Security & Privacy 1, no. 4 (2003): 77-82.
7. E. Leon, and S. D. Bruda. "Counter-measures against stack buffer overflows in GNU/Linux operating systems." Procedia Computer Science 83 (2016): 1301-1306.

Course Code					System and Network Security Laboratory					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
-	-	2	1	2	-	-	-	50	50	100

COURSE OBJECTIVES

- Study and Understand the Vulnerabilities exists in the system
- Carry out experiment with the memory structures in the system
- Understand and exhibit the hardware vulnerabilities
- Be familiar with the network security tools.

LIST OF EXPERIMENT

1.	**Buffer Overflow Attacks:** Implement buffer overflow to skip the execution of an instruction, buffer overflow to execute a script and start a shell.
2.	**Advanced Buffer Overflow Techniques:** Demonstrate Return-to-libc attack, Buffer overflow attack with Return Oriented Programming (ROP).
3.	**Other Security Vulnerabilities and Attacks:** Demonstrate Integer Overflow Vulnerability, Formatting string vulnerability attacks.
4.	**Advanced Security Concepts:** Study Hardware Trojans and their implications in security, Study and prepare a report on SSL design, focusing on its security features and vulnerabilities.
5.	**Network Security Analysis:** Run and analyze results from the Wireshark tool, focusing on network traffic, packet capture, and security analysis.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understand the consequences of buffer overflow attacks.
CO2- Experiment with the Formatting String exploits.
CO3- Demonstrate the Integer Overflow attacks.
CO4- Understand the prevention and mitigation techniques to withstand against hardware trojans.
CO5- Compare the security strength of network security protocols
CO6- Apply Packet sniffer tool to analyze the network communication.

TEXT/REFERENCE BOOKS

1. James Houston Baxter, “Wireshark Essentials”, Packt Publishing.
2. Dennis Andriesse, “Practical Binary Analysis”, No Starch Press.
3. Greg Hoglund, Gary McGraw, “Exploiting Software How to Break Code”, Addison-Wesley
4. Chris Anley, John Heasman, Felix Lindner, Gerardo Richarte, “The Shellcoder's Handbook Discovering and Exploiting Security Holes”, Wiley.
5. One, Aleph. "Smashing the stack for fun and profit." Phrack magazine.
6. B. Bierbaumer, K. Julian, K. Thomas, A.Francillon, and A. Zarras. "Smashing the stack protector for fun and profit." In ICT Systems Security and Privacy Protection: 33rd IFIP TC 11 International Conference, SEC 2018, Proceedings 33, pp. 293-306. Springer International Publishing, 2018.
7. D. Ahmad,. "The rising threat of vulnerabilities due to integer errors." IEEE Security & Privacy 1, no. 4 (2003): 77-82.
8. E. Leon, and S. D. Bruda. "Counter-measures against stack buffer overflows in GNU/Linux operating systems." Procedia Computer Science 83 (2016): 1301-1306.

Course Code					Blockchain-based Cyber Security					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	-	-	3	3	25	50	25	-	-	100

COURSE OBJECTIVES

- To understand the concepts of distributed consensus and trust management.
- To understand the design principles of the block chains.
- To design and implement the distributed ledger and the smart contracts.

UNIT 1: Introduction to Basics of Blockchain Introduction to Blockchain, Building blocks: SHA 256, Peer to Peer Network, Distributed Ledger, Block mining, Proof of work, Miners and incentive mechanisms, Merkle tree, case-study applications of block chain framework: Bitcoin and transactions.	**10 Hrs.**
UNIT 2:Distributed Consensus and Cryptocurrency Proof-of-Work based consensus mechanisms, Proof of Stake based Chains, Types of Blockchain, Introduction to Crypto Currency, Crypto Currency as application of blockchain technology.	**10 Hrs.**
UNIT 3: Ethereum Smart Contracts Ethereum Framework: Introduction, smart contract, Messages and transaction, state transition function, gas, applications, Solidity programming language: smart contract design, Rinkeby testnet.	**10 Hrs.**
UNIT 4: Cyber Security through Blockchain Technology Blockchain Use Cases for Cyber Security – Finance, Industry, E-Governance and other contract enforcement mechanisms. Security and Research Aspects in Blockchain.	**12 Hrs.**
	42 Hrs.

COURSE OUTCOMES

On completion of the course, students will be able to

CO1- Define the role of Blockchain technology in digitization.

CO2- Illustrate the cryptographic concepts, distributed concepts, and smart contracts related to Blockchain technology.

CO3- Identify the appropriate cryptographic primitives, type of Blockchain, mining method, and framework according to Blockchain use case.

CO4- Apply Ethereum framework for Blockchain development.

CO5- Analyze the need of Blockchain for real life system.

CO6- Design the smart contracts and Blockchain for suitable system.

TEXT/REFERENCE BOOKS

1. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction”, Princeton University Press
2. Emilia Balas Valentina, Ahmed A Elngar, Rajdeep Chakraborty, Anupam Ghosh, “Blockchain Principles and Applications in IoT”, CRC Press
3. White papers of Bitcoin, Ethereum, IOTA and Neo frameworks and research papers.
4. Gimenez-Aguilar, M., De Fuentes, J. M., Gonzalez-Manzano, L., & Arroyo, D. (2021). Achieving cybersecurity in blockchain-based systems: A survey. Future Generation Computer Systems, 124, 91-118.
5. Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2020). A systematic literature review of blockchain cyber security. Digital Communications and Networks, 6(2), 147-156.
6. Zhuang, P., Zamir, T., & Liang, H. (2020). Blockchain for cybersecurity in smart grid: A comprehensive survey. IEEE Transactions on Industrial Informatics, 17(1), 3-19.
7. Selvarajan, S., & Mouratidis, H. (2023). A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems. Scientific Reports, 13(1), 7107.

Course Code: XXXXXX					Scientific Writing and Publication Ethics					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs./Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
2	0	0	2	2	25	50	25	--	--	100

COURSE OBJECTIVES

1. To comprehend the significance of scientific writing and to understand of the basic structure of a scientific paper.
2. To get familiarize with the process of selecting appropriate target journals and conferences.
3. To cultivate an awareness of publication ethics within the realm of scientific writing.
4. To get acquainted with the knowledge and tools necessary to identify, understand, and avoid plagiarism in scientific writing

UNIT-1: Introduction to Scientific Writing Importance of scientific writing in engineering, understanding the structure and components of a scientific paper, research paper writing style, referencing style	**07 Hrs.**
UNIT 2: Selecting Target Journals and Conferences Types of journals and conferences in engineering, open access journals, journal impact factors, conference rankings, manuscript submission process, responding to reviewer comments	**07 Hrs.**
UNIT 3: Publication Ethics Introduction and importance, publication misconduct, violation of publication ethics, falsification and/or fabrication of data, understanding of copyright form, collaboration issues (authorship), conflicts of interest issues, Committee on Publication Ethics (COPE)	**07 Hrs.**
UNIT 4: Avoiding Plagiarism Plagiarism – definition, reasons for plagiarism, types of plagiarism, avoiding plagiarism	**07 Hrs.**
TOTAL	**28 Hrs**

COURSE OUTCOMES

On completion of the course, student will be able to:

CO1- Describe the importance of scientific writing in engineering and identifying its role in knowledge dissemination and academic integrity
CO2 - Understand the structure and components of a scientific paper
CO3 - Evaluate and select suitable journals and conferences to submit their research work
CO4 - Understand publication ethics
CO5 - Define plagiarism, identify its different types and reasons, and apply techniques to avoid plagiarism
CO6 - Analyze and respond to reviewer comments for their research work

TEXT/REFERENCE BOOKS

1. Getting It Published: A Guide for Scholars and Anyone Else Serious about Serious Books by William Germano
2. Publish and Flourish: Become a Prolific Scholar by Tara Gray
3. Adil E. Shamoo, and David B. Resnik, Responsible Conduct of Research, Oxford University Press
4. Gary Comstock, Research Ethics: A Philosophical Guide to the Responsible Conduct of Research, Cambridge University Press
5. Tony Mayer, and Nicholas H. Steneck, Promoting Research Integrity in a Global Environment, World Scientific Publishing
6. Ethical Issues in Engineering Research, Publication, and Practice by Caroline Whitbeck

2nd Semester

Course Code					Machine Learning for Cyber Security					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	-	-	3	3	25	50	25	-	-	100

COURSE OBJECTIVES

- To study the technical perspective of cybercrime.
- To understand the different Data Pre-processing operations.
- To discuss different Supervised and Unsupervised learning techniques.
- To understand the role of machine leaning in cyber forensics.

UNIT 1: Introduction to Machine Learning, Introduction to Machine Learning, Types of learning, Stages of Machine learning based system, Performance metric, Overfitting, Underfitting, Classification, and Regression, Ensemble Based Learning, Data set Collection, cleaning, visualization, and exploratory analysis, feature extraction.	**10 Hrs.**
UNIT 2: Threat Detection using Machine Learning Analysis of benchmark data, Threat classification, system logs, malware analysis, suspicious user behaviour, case Study on Intrusion Detection, difference between normal and malicious activity.	**12 Hrs.**
UNIT 3: Fraud and Spam Detection Introduction to common cyber fraud, feature engineering for identifying fraudulent patterns and behaviours, supervise learning approaches for fraud detections, Email Filtering, text-based feature extraction, behaviour analysis for spam detection.	**10 Hrs.**
UNIT 4: Deep Learning and Cyber Security Introduction to deep neural network, adversarial machine learning: adversarial attacks and defence, model interpretability in cyber security.	**10 Hrs.**
	42 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1 - Understand basics of machine learning.
CO2 - Identify the threat classification using machine learning.
CO3 - Select appropriate machine learning model for Intrusion detection system, fraud and anomaly detection.
CO4 - Apply feature selection methods for performance optimization.
CO5 - Design optimal machine learning models for cyber threat analysis.
CO6 - Evaluate machine learning algorithms in detecting and mitigating cyber threats.

TEXT/REFERENCE BOOKS

1. Aurélien Géron, “Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow”, O'Reilly Media
2. Tom Mitchell, “Machine Learning”, Mc Graw Hill
3. Sebastian Raschka, Vahid Mirjalili, “Machine Learning and Deep Learning with Python, Scikit-learn, and TensorFlow 2”, Packt Publishing
4. Jagannath E. Nalavade, “Machine Learning Approaches in Cyber Security”, Namya Press Publisher
5. Soma Halder, Sinan Ozdemir, “Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem”, Packt Publishing

RESEARCH PAPERS

1. Giovanni Apruzzese et al., “The Role of Machine Learning in Cybersecurity”, Digital Threats: Research and Practice. Doi: https://doi.org/10.1145/3545574
2. M. Wazi dwt al., Uniting cyber security and machine learning: Advantages, challenges and future research”, ICT Express. Doi: https://doi.org/10.1016/j.icte.2022.04.007
3. Z. Azam et al., “Comparative Analysis of Intrusion Detection Systems and Machine Learning-Based Model Analysis Through Decision Tree, IEEEAccess. Doi: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10185955

PREREQUISITES:

Course Code					Machine Learning for Cyber Security Laboratory					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
0	0	2	1	2	-	-	-	50	50	100

Pandit Deendayal Energy University School of Technology

- Basic knowledge of linear algebra, probability and statistics. Familiarity with programming languages such as Python.

COURSE OBJECTIVES

- To familiarize students with basic machine learning techniques and their application in cybersecurity.
- Discuss different Supervised and Unsupervised learning techniques.
- To provide students with practical experience in applying machine learning techniques to real-world cybersecurity datasets.

LIST OF EXPERIMENT

1.	**Data Exploration and Preprocessing**: Data exploration using Pandas and NumPy, Preprocessing of datasets, including handling missing values, scaling, encoding categorical variables, etc.
2.	**Supervised Learning Models**: Linear and Non-linear Regression, Classification Models (KNN, SVM, Naïve Bayes, Decision Tree, Logistic Regression), Ensemble Techniques (Random Forests, Gradient Boosting), Neural Network Architecture using TensorFlow or PyTorch, Hyperparameter Tuning for various machine learning algorithms
3.	**Unsupervised Learning and Anomaly Detection**: Network Traffic Anomaly Detection using Clustering Algorithms (K-Means, Hierarchical Clustering, DBSCAN), Phishing Email Dataset Analysis using Clustering Algorithms
4.	**End-to-End Machine Learning Pipeline for Cybersecurity**: Designing and implementing an end-to-end pipeline encompassing data preprocessing, model training, hyperparameter tuning, and evaluation using real-world cybersecurity datasets
5.	**Adversarial Attacks and Model Security**: Implementing adversarial attacks (FGSM, PGD) on trained models for malware detection, Understanding and defending against adversarial attacks to ensure model security
6.	**Performance Evaluation and Comparative Analysis**: Evaluating the performance of various machine learning models on cybersecurity tasks, Comparing the effectiveness of different algorithms and techniques in detecting and preventing cybersecurity threats

COURSE OUTCOMES

On completion of the course, students will be able to

CO1 - Understand basic machine learning concepts.
CO2 - Implement supervised and unsupervised algorithms for cybersecurity tasks.
CO3 - Apply data pre-processing operations for data cleaning and feature selection.
CO4 - Implement deep learning models for cybersecurity tasks.
CO5 - Analyze the results of machine learning models in cybersecurity.
CO6 - Build machine learning-based solutions for Cyber Security.

TEXT/REFERENCE BOOKS

1. Aurélien Géron, “Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow”, O'Reilly Media, Inc.
2. Sebastian Raschka, Vahid Mirjalili, “Machine Learning and Deep Learning with Python, Scikit-learn, and TensorFlow”, Packt Publishing
3. Jagannath E. Nalavade, “Machine Learning Approaches in Cyber Security”, Namya Press
4. Soma Halder, Sinan Ozdemir, “Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem”,Packt Publishing

RESEARCH PAPERS

1. Z. Azam et al., “Comparative Analysis of Intrusion Detection Systems and Machine Learning-Based Model Analysis Through Decision Tree, IEEEAccess. Doi:
https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10185955
2. N. Shone et al. “A Deep Learning Approach to Network Intrusion Detection”, IEEE Transactions on Emerging Topics in Computational Intelligence.

Course Code: XXXXXX					Research Methodology					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs./Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
2	0	0	2	2	25	50	25	--	--	100

COURSE OBJECTIVES

1. To understand the role of research in the field of engineering and get an overview of the research process.
2. To develop proficiency in literature review techniques.
3. To understand the process of formulating and solving research problems.
4. To understand different types of intellectual property rights.

UNIT I : Introduction to Research Role of research in engineering, research process overview, types of research, outcomes of research, characteristics of a researcher, research terminology	**06 Hrs.**
UNIT II : Literature Review Techniques Searching for the existing literature, reviewing the selected literature, developing a theoretical framework, developing a conceptual framework	**06 Hrs.**
UNIT III : Formulating and Solving a Research Problem Importance of formulating a research problem, sources of research problems, identifying a problem, formulation of research objectives and research questions, Need for research design, different research designs, experimental test-setups, data sampling, data collection, data analysis & interpretation	**08 Hrs.**
UNIT VI: Intellectual Property Rights Introduction and significance of intellectual property rights, types of intellectual property rights, introduction to patents, patent drafting and filing, copyright, trademarks, industrial design, geographical indicators	**08 Hrs.**
Total	**28 Hrs.**

COURSE OUTCOMES

On completion of the course, student will be able to:

CO1 - Understand the role and significance of research in engineering
CO2 - Develop understanding of the basic framework of research process and design
CO3 - Identify technical gaps in the literature and formulate a problem.
CO4 - Develop an understanding of various research designs and techniques.
CO5 - Develop an understanding of the ethical dimensions of conducting applied research
CO6 - Evaluate and apply intellectual property rights concepts to the research outcomes

TEXT/REFERENCE BOOKS

1. Stuart Melville, Wayne Goddard, Research Methodology: An Introduction for Science and Engineering Students, Juta & Co. Ltd.
2. David V. Thiel, Research Methods for Engineers, Cambridge University Press, UK
3. Ranjit Kumar, Research Methodology: A Step by Step Guide for Beginners, Pearson
4. CR Kothari, Research Methodology (Methods and Techniques), New age Publications

Course Code					Web Security and Penetration Testing					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	--	--	100

COURSEOBJECTIVES

- To understand the concepts and methodologies of web penetration testing.
- To learn about web application security.
- To learn various web application vulnerabilities and exploitation techniques.
- To develop skills for performing web penetration testing.

UNIT 1:Introduction to Web Application Security Introduction to security in web applications and common web application vulnerabilities Web architecture and protocols: Understanding how web applications work, including HTTP requests and responses, cookies, sessions, and other web-related concepts; Web application technologies; Information gathering techniques.	**10 Hrs.**
UNIT 2: Active Enumeration and Vulnerability Identification Active enumeration for gathering information: Port scanning, checking username validity, Brute forcing usernames, enumerating files, Brute forcing passwords, gathering other information from web pages; Identifying vulnerability: Automated URL-based directory traversal, automated cross-site scripting, query checking; Case studies.	**11 Hrs.**
UNIT 3: Web SQL Injection and Header Manipulation SQL Injection: Checking jitter, URL-based SQL injection, blind SQL injection, encoding payloads; Web Header Manipulation: Fingerprinting servers, testing for insecure headers, brute forcing login; testing for insecure cookie flags; session fixation through cookie injection; Case studies.	**11 Hrs.**
UNIT 4: Steganography, Encryption and Encoding in Websites Image Analysis and Manipulation: Hiding a message by steganography, extracting the hidden message, hiding text in image, extracting text from images, command and control by using steganography; Encryption and Encoding: Encoding with different techniques, cracking different ciphers, attacking one-time pad reuse; Case studies.	**10 Hrs.**
	42 Hrs.

COURSEOUTCOMES

On completion of the course, student will be able to

CO1 - Understand security concerns in web applications.

CO2 - Illustrate the concepts and methodologies for penetration testing of a web application.

CO3 - Evaluate the security of a web application.

CO4 - Identify and exploit common web application vulnerabilities.

CO5 - Apply the testing framework to conduct web penetration testing.

CO6 – Develop effective mitigation strategies to secure web applications.

TEXT/REFERENCE BOOKS

1. Dafydd Stuttard (Author), Marcus Pinto, "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws", Wiley.
2. Prakhar Prasad: "Mastering Modern Web Penetration Testing", Packt Publishing Limited.
3. Bryan Sullivan and Vincent Liu,"Web Application Security: A Beginner's Guide", McGraw-Hill.
4. Cameron Buchanan, Terry Ip, Andrew Mabbitt, Benjamin May, Dave Mound , “Python Web Penetration Testing Cookbook”, Packt Publishing Limited.

RESEARCH PAPERS

1. P. A. E. Pratama and A. M. Rhusuli, "Penetration Testing on Web Application Using Insecure Direct Object References (IDOR) Method," 2022 International Conference on ICT for Smart Society (ICISS), Bandung, Indonesia, 2022, pp. 01-07, doi: 10.1109/ICISS55894.2022.9915074.
2. . E. López de Jiménez, "Pentesting on web applications using ethical - hacking," 2016 IEEE 36th Central American and Panama Convention (CONCAPAN XXXVI), San Jose, Costa Rica, 2016, pp. 1-6, doi: 10.1109/CONCAPAN.2016.7942364.

Course Code					Web Security and Penetration Testing Laboratory					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
0	0	2	1	2	--	--	--	50	50	100

COURSEOBJECTIVES

- To understand the concepts and methodologies of web penetration testing.
- To learn about web application security.
- To learn various web application vulnerabilities and exploitation techniques.
- To develop skills for performing web penetration testing.

LIST OF EXPERIMENTS

1.	**Information Gathering:** Working with HTTP requests and responses, cookies, sessions Gathering other information from web pages
2.	**Password Cracking:** Brute forcing passwords Dictionary Attack
3.	**Web Based Attacks:** Automated cross-site scripting URL-based SQL injection Implement blind SQL injection attacks against web applications with input validation mechanisms. Develop and execute advanced cross-site scripting (XSS) attacks, including DOM-based XSS and XSS via AJAX. Conduct session fixation attacks to set session IDs and subsequently hijack active sessions. Create CSRF exploits to trick authenticated users into performing unintended actions on a web application.
4.	**Web Application Threat Mitigation:** Generate/Implement different hashes Text/Image Steganography in Websites Encoding with different techniques for Websites Implementing an existing research work on web pen testing
5.	**Case studies on web penetration testing.**
6.	**Mini Project**

COURSE OUTCOMES

On completion of the course, student will be able to

CO1 - Recall basic concepts of web applications.
CO2 - Understand the mechanisms behind common web vulnerabilities and their potential impact.
CO3 - Implement techniques for gathering information from web pages.
CO4 - Analyze different penetration techniques for web applications.
CO5 - Evaluate the reliability and validity of existing research works on web pen testing.
CO6 - Develop strategies for implementing and testing web application security measures.

TEXT/REFERENCE BOOKS

1. Dafydd Stuttard (Author), Marcus Pinto, "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws", Wiley.
2. Prakhar Prasad: "Mastering Modern Web Penetration Testing", Packt Publishing Limited.
3. Bryan Sullivan and Vincent Liu,"Web Application Security: A Beginner's Guide", McGraw-Hill.
4. Cameron Buchanan, Terry Ip, Andrew Mabbitt, Benjamin May, Dave Mound , “Python Web Penetration Testing Cookbook”, Packt Publishing Limited.

Course Code					Cyber Physical System Security					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	-	-	100

COURSE OBJECTIVES

- To learn about the security issues in IoT and cloud computing.
- To learn about the cryptography solutions and issues in IoT.
- To learn about the security measures taken in IoT and Cloud systems to improve security.

UNIT 1: Introduction to CPS Definition of CPS, characteristics, applications, challenges, security considerations in CPS, sensors, actuators, controllers and feedback loops, Introduction to Industrial Control Systems and Operations, Industrial Network Protocols, Cyber Physical System Modelling.	**12 Hrs.**
UNIT 2: Secure Design for CPS Vulnerabilities in control systems: Physical attacks, sensors/actuators spoofing, network-based attacks, hardware, and software security: Secure boot, trusted computing platform, risk assessment and threat modeling.	**10 Hrs.**
UNIT 3: Secure Communication Network in CPS Secure communication protocols, network zone in CPS, WSN security: node compromise, jamming attack, localization attack, cryptographic techniques for WSN.	**10 Hrs.**
UNIT 4: Defence Mechanisms in CPS and Advanced Application DDoS attack, sensor tempering, data injection attacks, manipulation of control signals, IDPS for CPS, CPS Applications on Power Grid, Railways Systems, Transportation Systems.	**10 Hrs.**
	42 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1 - Understand the concepts and security challenges in CPS.
CO2 - Identify vulnerabilities in control systems.
CO3 - Analyze physical and network attacks in CPS.
CO4 - Evaluate secure communication protocols in CPS infrastructure.
CO5 - Demonstrate defence mechanisms such as DDoS attack, sensor tempering, data injection attacks, manipulation of control signals, IDPS for CPS.
CO6 - Analyze case studies related to CPS infrastructures.

TEXT/REFERENCE BOOKS

1. Sajal K. Das, Krishna Kant, Nan Zhang, Morgan Kaufmann, “Handbook on Securing Cyber-Physical Critical Infrastructure”, Elsevier
2. Houbing Song, Glenn A. Fink, Sabina Jeschke, “Security and Privacy in Cyber-Physical Systems”, Wiley-IEEE Press.
3. Dibaji, Seyed Mehran, Mohammad Pirani, David Bezalel Flamholz, Anuradha M. Annaswamy, Karl Henrik Johansson, and Aranya Chakrabortty. "A systems and control perspective of CPS security." Annual reviews in control 47 (2019): 394-411.
4. Keerthi, Ch Krishna, M. A. Jabbar, and B. Seetharamulu. "Cyber physical systems (CPS): Security issues, challenges and solutions." In 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pp. 1-4. IEEE, 2017.

Course Code					Cyber Threat Intelligence					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	-	-	100

COURSE OBJECTIVES

- Understand the six phases of the threat intelligence life cycle and apply them to evaluate cyber threat intelligence.
- Classify various attack vectors used by threat actors to target organizations.
- Define methods for extracting threat intelligence from social media, the deep web, and the dark web to assist in financial crime investigations.
- Develop risk assessments that address specific cyber threats impacting the financial sector.
- Apply threat intelligence analysis techniques to identify and mitigate cyber threats effectively.

UNIT 1: Introduction to Cyber Threat Intelligence and the Threat Intelligence Life Cycle Overview of cyber threat intelligence concepts and importance, The six phases of the threat intelligence life cycle: Planning and Direction, Collection, Processing and Analysis, Dissemination, Integration, and Feedback, Ethical and legal considerations in cyber threat intelligence practices.	**10 Hrs.**
UNIT 2: Attack Vectors, Threat Actors, and Extracting Threat Intelligence Classification of attack vectors (e.g., malware, phishing, insider threats), Analysis of threat actor profiles and motivations, Methods for extracting threat intelligence from social media platforms, Techniques for monitoring the deep web and dark web for cyber threat indicator.	**11 Hrs.**
UNIT 3: Threat Intelligence Analysis and Practical Applications Application of threat intelligence analysis techniques, Hands-on exercises and labs to apply threat intelligence analysis techniques, Analysis of real-world case studies and incidents, Discussion on best practices and lessons learned from cyber threat intelligence operations.	**11 Hrs.**
UNIT 4: Risk Assessment and Mitigation Strategies in the Financial Sector Overview of risk assessment methodologies (e.g., NIST Cybersecurity Framework, FAIR), Application of risk assessment techniques to identify and prioritize cyber threats impacting the financial sector, Development of risk assessment reports and recommendations, cyber threats in the financial sector.	**10 Hrs.**
	42 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understanding key terminology and principles associated with the threat intelligence life cycle, attack vectors, threat actors, and risk assessment.

CO2- Recognizing the processes and phases involved in the threat intelligence life cycle.

CO3- Apply classification schemes to categorize different types of attack vectors and threat actors.

CO4- Analyse the potential impact of different attack vectors and threat actor behaviors on organizational security.

CO5- Create cyber threat intelligence-driven strategies to address specific cyber threats and vulnerabilities.

CO6- Evaluate the effectiveness of threat intelligence analysis techniques in identifying and mitigating cyber threats.

TEXT/REFERENCE BOOKS

1. Rebekah Brown, Scott J: Intelligence-Driven Incident Response, O'Reilly.
2. Matthew Pepe, Jason T. Luttgens and Kevin Mandia: Incident Response & Computer Forensics, McGraw Hill.
3. Online resources and tutorials on specific security topics.

RESEARCH PAPER

1. Rosa, R. Batista, R. Gonçalves, J. Martins and F. Branco, "Cyber Threat Intelligence Architecture for Applied Cybersecurity Scenarios: PhD Thesis Proposal in Web Science and Technology," 2022 17th Iberian Conference on Information Systems and Technologies (CISTI), Madrid, Spain, 2022, pp. 1-6,
2. F. K. Kaiser, L. J. Andris, T. F. Tennig, J. M. Iser, M. Wiens and F. Schultmann, "cyber threat intelligence enabled automated attack incident response," 3rd international conference on next generation computing applications (nextcomp).

Course Code					Social Network Security and Privacy					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	--	--	100

COURSE OBJECTIVES

- To develop semantic web related simple applications
- To explain Privacy and Security issues in Social Network.
- To discuss the prediction of human behaviour in social communities.
- To describe the Access Control, Privacy and Security management of social networks.

UNIT 1: Fundamentals of Social Networks Introduction to Semantic Web, Limitations of current Web, Development of Semantic Web, Emergence of the Social Web, Social Network analysis, Development of Social Network Analysis, Key concepts and measures in network analysis, Historical overview of privacy and security, Major paradigms for understanding privacy and security.	**10 Hrs.**
UNIT 2: Security Issues in Social Networks The evolution of privacy and security concerns with networked technologies, Contextual influences on privacy attitudes and behaviours, Anonymity in a networked world.	**10 Hrs.**
UNIT 3: Predicting Human Behaviour and Privacy Issues Understanding and predicting human behaviour for social communities, User data Management, Inference and Distribution, Enabling new human experiences, Reality mining, Context, Awareness, Privacy in online social networks, Trust in online environment, Neo4j, Nodes, Relationships, Properties.	**10 Hrs.**
UNIT 4: Access Control, Privacy and Identity Management Understand the access control requirements for Social Network, Enforcing Access Control Strategies, Authentication and Authorization, Roles-based Access Control, Host, storage and network access control options, Firewalls, Authentication, and Authorization in Social Network, Identity & Access Management, Single Sign-on, Identity Federation, Identity providers and service consumers, The role of Identity provisioning.	**12 Hrs.**
	42 Hrs.

COURSE OUTCOMES

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

CO1 - Understand fundamental concepts and historical background of social networks.

CO2 - Comprehend the evolution of privacy and security concerns in networked technologies.

CO3 - Apply knowledge of network analysis concepts to analyze and interpret social network data.

CO4 - Analyze the implications of user data management, inference, and distribution on privacy in online social networks.

CO5 - Evaluate the impact of social network analysis techniques on predicting human behaviour in social communities.

CO6 - Create comprehensive access control policies and identity management frameworks tailored to the specific needs and challenges of social networks.

TEXT/REFERENCE BOOKS

1. Peter Mika, “Social Networks and the Semantic Web”, Springer.
2. Borko Furht, “Handbook of Social Network Technologies and Application”, Springer.
3. Jérôme Baton and Rik Van Bruggen - Learning Neo4j 3.x, Packt publishing.
4. David Easley and Jon Kleinberg - Networks, Crowds, and Markets: Reasoning about a Highly Connected World, Cambridge University Press.

REFERENCE PAPERS:

1. Mislove, A., Viswanath, B., Gummadi, K. P., & Druschel, P. (2010). Privacy in Social Networks: How Risky is Your Social Graph? ACM Transactions on the Web (TWEB), 4(1), 1-22.
2. Ferrari, E., & Demartini, G. (2012). A Survey of Security and Privacy Issues in Social Networks. IEEE Transactions on Dependable and Secure Computing (TDSC), 9(4), 561-576.
3. Limonad, L., Elovici, Y., Shapira, B., & Shahar, Y. (2015). Social Network Security: Issues, Challenges, and Future Directions. ACM Transactions on Internet Technology (TOIT), 15(2), 1-25.
4. Ray, I., & Ray, I. (2016). A Survey on Social Network Security Issues. ACM Computing Surveys (CSUR), 49(3), 1-36.

Course Code					Advanced Topics in Cryptography					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	-	-	100

COURSE OBJECTIVES

- To study of advanced encryption techniques
- To study of access control policies and mechanisms
- To study of quantum cryptography

UNIT 1: Homomorphic encryption Overview, Need of homomorphic encryption, components: encryption, key generation, operations, decryption. Security assumptions. Partial and fully.	**10 Hrs.**
UNIT 2: Identity and Attribute Based Cryptography Role Based Access Control, Boneh's scheme for identity-based encryption, Goyal's scheme for Attribute Based cryptography, Extensions: multi authority, hidden access structure, constant length ciphertext	**10 Hrs.**
UNIT 3: Functional Encryption and Secure Multi-Party Communication Function encryption, components and varieties for function encryption, Overview of MPC and its applications, Yao's garbled circuits, Secret sharing schemes	**12 Hrs.**
UNIT 4: Post Quantum Cryptography Overview, primitives: Hash-based, lattice-based, code-based, and multivariate-based schemes Quantum-resistant cryptographic protocols, NIST post-quantum cryptography standardization efforts	**10 Hrs.**
	42 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1-Understand homomorphic cryptographic algorithms and their security properties.
CO2- Illustrate identity based cryptographic protocols for privacy, integrity, and authentication.
CO3- Analyze attribute based cryptographic solutions.
CO4- Evaluate the security of quantum cryptographic systems.
CO5- Explore emerging trends and challenges in advanced cryptography.
CO6- Create solutions for cryptography challenges for real-world applications.

TEXT/REFERENCEBOOKS

1. William Stallings "Cryptography and Network Security: Principles and Practice" by Peasron.
2. Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen "Post-Quantum Cryptography" by Springer.
3. Research papers and articles from cryptographic conferences and journals (e.g., Crypto, Eurocrypt, ACM CCS).

RESEARCH PAPER

1. John Bethencourt, Amit Sahai, and Brent Waters. "Ciphertext-policy attribute-based encryption." In 2007 IEEE symposium on security and privacy (SP'07), pp. 321-334. IEEE, 2007.
2. Bernstein, Daniel J., and Tanja Lange. "Post-quantum cryptography." Nature 549.7671 (2017): 188-194.
3. Capocelli, Renato M., et al. "On the size of shares for secret sharing schemes." Journal of Cryptology 6.3 (1993): 157-167.
4. Yang, Kang, et al. "Attribute Based Encryption with Efficient Revocation from Lattices." Int. J. Netw. Secur. 22.1 (2020): 161-170.

Course Code : PG_CS_2					Advanced Topics in Cryptography Laboratory					
Teaching Scheme					Examination Scheme					
					Theory			Practical		Total Marks
L	T	P	C	Hrs/Week	MS	ES	IA	LW	LE/Viva	
0	0	2	1	2	-	-	-	25	25	50

COURSE OBJECTIVES

- To investigate the principles and applications of homomorphic encryption within the advanced cryptography laboratory setting.
- To explore the concepts of function encryption and role-based access control in the context of cryptography practical implementation.
- To examine the theoretical underpinnings and potential practical implications of quantum cryptography through experimentation and analysis within the laboratory environment.

LIST OF EXPERIMENTS

1.	**Cryptography algorithms** Implementation of Ciphers, Advanced Encryption System, Data Encryption System, RSA, Diffie–Hellman, SHA, NIST standards.
2.	**Identity based encryption** Implementation of Setup, Keygen, Encrypt and Decrypt.
3.	**Attribute based encryption** Implementation of Single authority, Multi authority.
4.	**Functional encryption** Implementation of Encryption, Decryption.
5.	**Quantum cryptography** Study of Qbit implementation, Encryption, Decryption.
6.	**Homomorphic Encryption** Study of operations in homomorphic encryption
7.	**Mini Project**

COURSE OUTCOMES

On completion of the course, student will be able to

CO1-Understand advanced cryptographic algorithms and their security properties.
CO2- Apply identity based cryptographic protocols for privacy, integrity, and authentication.
CO3- Implement attribute based cryptographic solutions for real-world applications.
CO4- Evaluate the security of homomorphic cryptographic systems.
CO5- Implement concepts of quantum cryptography.
CO6- Develop solutions using advanced cryptographic algorithms to solve complex problems.

TEXT/REFERENCE BOOKS

1. William Stallings "Cryptography and Network Security: Principles and Practice", Pearson.
2. Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen "Post-Quantum Cryptography", Springer.
3. Research papers and articles from cryptographic conferences and journals (e.g., Crypto, Eurocrypt, ACM CCS).

Course Code					Data Authorization and Privacy Preservation					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	-	-	3	3	25	50	25	-	-	100

COURSE OBJECTIVES

- Determine key concepts of data security, authentication, and authorization.
- Study the social, and legal aspects of data privacy and its impact on new emerging technologies.
- Examine real-world - problems that requires data privacy ad anonymization.

UNIT 1:Introduction Authentication Vs Authorization, Methods of Authentications: Password based authentication, Biometric Authentication, Multi-factor Authentication. Data Access Control Methods: **Discretionary access control (DAC), Mandatory Access Control, Role Based Access Control, Attribute-based access control, Identity and Access Management (IAM).**	**12 Hrs.**
UNIT 2:Data Privacy Threat and Challenges Understanding Privacy: Social Aspects of Privacy Legal Aspects of Privacy and Privacy Regulations, Effect of Database and Data Mining technologies on privacy challenges raised by new emerging technologies such RFID, biometrics, etc.,	**8 Hrs.**
UNIT 3:Data Privacy Models Privacy Models, Introduction to Anonymization, Anonymization models: K-anonymity, l-diversity, t-closeness, differential privacy, Database as a service	**12 Hrs.**
UNIT 4:Data Privacy For Data Science Using technology for preserving privacy. Statistical Database security Inference Control, Secure Multi-party computation, Privacy-preserving Data mining, Hippocratic databases, Emerging Applications: Social Network Privacy, Location Privacy, Query Log Privacy, Biomedical Privacy	**10 Hrs.**
	42 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understand the security issues related with data privacy.

CO2- Differentiate between authentication and authorization concepts.

CO3- Evaluate the security strength and weakness of access control mechanisms such as single factor and multifactor authentication.

CO4- Compare the trade-offs between privacy and accuracy amongst existing anonymization models.

CO5- Identify the key technologies used for privacy preservation

CO6- Present and critically assess current research on data security, privacy preservation and anonymization.

TEXT/REFERENCE BOOKS

1. Sirapat Boonkrong, Authentication and Access Control: Practical Cryptography Methods and Tools, APress Publication
2. Elena Ferrari, Access Control in Data Management Systems, Morgan & Claypool Publishers
3. Sweeney, Latanya. "k-anonymity: A model for protecting privacy." International journal of uncertainty, fuzziness and knowledge-based systems 10.05 (2002): 557-570.
4. Machanavajjhala, Ashwin, et al. "l-diversity: Privacy beyond k-anonymity." Acm transactions on knowledge discovery from data (tkdd) 1.1 (2007): 3-es.
5. Li, Ninghui, Tiancheng Li, and Suresh Venkatasubramanian. "t-closeness: Privacy beyond k-anonymity and l-diversity." 2007 IEEE 23rd international conference on data engineering. IEEE, 2006.
6. Domingo-Ferrer, Josep, and Jordi Soria-Comas. "From t-closeness to differential privacy and vice versa in data anonymization." Knowledge-Based Systems 74 (2015): 151-158.

Course Code					Security Protocols					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	-	-	100

COURSE OBJECTIVES

- To study application security applications
- To study privacy enhanced protocols
- To study security protocol infrastructure

UNIT 1: Introduction Introduction of security protocols, study of differential privacy, Various mitigation techniques in privacy and security mechanisms in protocols, Secure Messaging Protocols	**10 Hrs.**
UNIT 2: Privacy Enhanced Protocols TOR (The Onion Router), Proxy Re-encryption techniques, Security risk in the protocols, Private information retrieval	**10 Hrs.**
UNIT 3: Contract-Signing Protocols Fundamental limitation of Contract-Signing and Fair-Exchange, Trusted third party, Optimistic Contract-Signing, Asokan-Shoup-Waidner protocol, Desirable properties (fairness, timeliness, accountability, balance), Abuse-Free Contract-Signing	**10 Hrs.**
UNIT 4: Protocol Analysis and Verification Logic for Computer Security Protocols: Floyd-Hoare logic of programs, BAN Logic, Compositional Logic for Proving Security Properties of Protocols. Symbolic Protocol Analysis: Strand space model, Symbolic analysis problem, From protocols to constraints, SRI Constraint Solver. Protocol Verification by the induction methods, Game-Based Verification of Fair Exchange Protocols	**12 Hrs.**
	42 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to
CO1-Understand fundamental concepts of security protocols.
CO2-Analyze and evaluate privacy in the security protocols.
CO3-Design and implement contract signing protocols.
CO4-Apply security protocols to real-world scenarios.
CO5-Assess security risks and vulnerabilities in protocols.
CO6-Develop a system with secure architecture.

TEXT/REFERENCEBOOKS

1. William Stallings, "Cryptography and Network Security: Principles and Practices", Pearson Publisher.
2. Ross Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems" by WILEY.
3. Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C" by WILEY.

Course Code					Hardware Security					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	-	-	100

COURSE OBJECTIVES

- To understand fundamental concepts of hardware security.
- To gain understanding cryptographic techniques to secure hardware designs.

UNIT 1: Introduction and Cryptographic Primitives to Hardware Security Overview of hardware security concepts and challenges, Importance of hardware security, Threat models and attack vectors in hardware systems, Case studies of real-world hardware security breaches, Key management and distribution in hardware systems, Cryptographic protocols for secure communication in hardware.	**10 Hrs.**
UNIT 2: Secure hardware design Trusted Platform Modules (TPMs) and secure boot, Hardware-based root of trust, Secure enclave architectures (e.g., Intel SGX, ARM TrustZone), Side-channel leakage models, Countermeasures against side-channel attacks in hardware designs, Case studies of side-channel attacks on real-world systems, Techniques for verifying the security of hardware designs, Formal verification methods, Hardware security testing and evaluation, Compliance standards and certifications for secure hardware, IOT Security	**11 Hrs.**
UNIT 3: Hardware Trojans, Physical attacks and Counterfeit Hardware Detection and prevention techniques for hardware Trojans, Supply chain security in hardware manufacturing, Techniques for detecting counterfeit hardware components, Tamper resistance techniques, Secure encapsulation and packaging, Case studies of physical attacks on hardware. Embedded Security	**11 Hrs.**
UNIT 4: Emerging Trends in Hardware Security Overview of recent advancements and research in hardware security, Future challenges and opportunities in hardware security, Ethical considerations in hardware security research and practice.	**10 Hrs.**
	42 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understand the fundamental principles of hardware security, including the threats and vulnerabilities unique to hardware components.

CO2- Identify different types of hardware attacks, such as side-channel attacks, fault injection attacks, and hardware Trojans.

CO3- Analyze the security implications of hardware design choices, including the impact of hardware security on system integrity and confidentiality.

CO4- Design and implement secure hardware systems, considering principles such as secure bootstrapping, secure key management, and hardware-based attestation.

CO5- Explore emerging trends and challenges in hardware security.

CO6- Evaluate existing hardware security mechanisms and countermeasures, including cryptographic techniques, secure boot protocols, and hardware obfuscation methods.

TEXT/REFERENCE BOOKS

1. Mohammad Tehranipoor, Cliff Wang, "Introduction to Hardware Security and Trust", Springer
2. Mohammad Tehranipoor, Cliff Wang, "Principles of Hardware Security", Springer
3. Research papers and articles from relevant conferences and journals (e.g., IEEE Transactions on Information Forensics and Security, ACM Transactions on Embedded Computing Systems).
4. Online resources and tutorials on specific hardware security topics.

Reference papers:

1. Hu, W., Chang, C., Sengupta, A., Bhunia, S., Kastner, R. & Li, H. (2020). An overview of hardware security and trust : threats, countermeasures and design tools. IEEE Transactions On Computer-Aided Design of Integrated Circuits and Systems. https://dx.doi.org/10.1109/TCAD.2020.3047976
2. Wachsmann, C., Sadeghi, AR. (2015). Basics of Physically Unclonable Functions. In: Physically Unclonable Functions (PUFs). Synthesis Lectures on Information Security, Privacy, and Trust. Springer, Cham. https://doi.org/10.1007/978-3-031-02344-6_2
3. Oh, S.-R.; Seo, Y.-D.; Lee, E.; Kim, Y.-G. A Comprehensive Survey on Security and Privacy for Electronic Health Data. *Int. J. Environ. Res. Public Health* **2021**, *18*, 9668. https://doi.org/10.3390/ijerph18189668