M. Tech.

Computer Science and Engineering

(CSE)

with specialization in

Information Security and Privacy

Department of Computer Science and Engineering

M.Tech. Computer Science and Engineering with specialization in Information Security and Privacy

Sr. No.	Subject	Code	Scheme L-T-P	Exam Scheme			Credits (Min.)	Notional hours of Learning (Approx.)
				Th. Marks	T Marks	P Marks		
	First Semester							
1	Mathematical Foundations of Information Security (Core – 1)	CSIS101	3-1-0	100	25	0	4	70
2	Design and Analysis of Algorithms (Core – 2)	CSIS103	3-0-2	100	0	50	4	85
3	Principles of Information Security and Privacy (Core – 3)	CSIS105	3-0-2	100	0	50	4	85
4	Core Elective -1	CSIS1XX	3-1-0 / 3-0-2	100	0 / 25	0 / 50	4	70 / 85
5	Core Elective - 2	CSIS1XX	3-0-2	100	0	50	4	85
						Total	**20**	**395 - 410**
6	Vocational Training / Professional Experience (Optional) (Mandatory for Exit)	CSISV91 CSISP93	0-0-10				5	200 (20 x 10)
	Second Semester							
1	Information Theory and Coding (Core – 4)	CSIS102	3-1-0	100	25	0	4	70
2	Network Security (Core – 5)	CSIS104	3-0-2	100	0	50	4	85
3	Elective - 3	CSIS1XX	3-1-0 / 3-0-2	100	0 / 25	0 / 50	4	70 / 85
4	Elective - 4	CSIS1XX	3-0-2	100	0	50	4	85
5	Institute Elective*	CSIS1XX	3-0-0 / 3-0-2 / 3-1-0	100	0 / 25	0 / 50	3 / 4	55 / 70 / 85
6	Mini Project	CSIS106	0-0-4	-	-	100	2	70
						Total	**21 – 22**	**435 - 480**
7	Vocational Training / Professional Experience (Optional) (Mandatory for Exit)	CSISV92 CSISP94	0-0-10				5	200 (20 x 10)
	Third Semester							
1	MOOC course – I*	Φ	-	-	-	-	3 / 4	70 / 80
2	MOOC course – II*	Φ	-	-	-	-	3 / 4	70 / 80
3	Dissertation Preliminaries	CSIS295	-	-	-	350$	14	560
						Total	**20 - 22**	**700 - 720**
	Fourth Semester							
1	Dissertation	CSIS296	-	-	-	600$	20	800
						Total	**20**	**800**

Sardar Vallabhbhai National Institute of Technology (SVNIT) Surat
Department of Computer Science and Engineering
M.Tech. Information Security and Privacy (Curriculum and Syllabus 2024-25)

L: Lecture; T: Tutorial; P: Practical; Th: Theory
*****to be offered to the PG students of other department and other PG Programs with the department.
Subject Code: Core, Electives, Dissertation Preliminary and Dissertation: **$$##nXX;** Vocational Training: **$$##VXX;** Professional Experience: **$$##PXX; $$:** Department Name; **##**: M.Tech Course Identity; **n**: Year; **XX**: Core (01 to 10), Elective (11 to 70), Institute Elective (71 to 90), Vocational Training (91 to 92), Professional Experience (93 to 94), Dissertation Preliminary (95), Dissertation (96), XX last digit odd number (for odd semester); XX last digit even number (for even semester)
Calculation of Notional Hours for the subject containing Theory, Tutorial and Practical Example: 3-1-2: 3*15+1*15+2*15+10 (Exam)= 100
$ **Internal**: 40% and **External**: 60%, *Swayam/NPTEL, ϕ As per 66th IAAC, Dated 20th March, 2024, Resolution No. 66.34 and 61st Senate resolution No. 4, 25th April, 2024.

Code	Elective Subjects	Scheme
	Core Elective 1 and 2	
CSIS111	Modern Cryptography	3-1-0
CSIS113	Cloud Computing and Big Data Analytics	3-0-2
CSIS115	Machine Learning	3-0-2
CSIS117	Cyber Physical Systems	3-0-2
CSIS119	Digital Forensics	3-0-2
CSIS121	Defensible Security Architectures	3-0-2
CSIS123	Research Methodology in CSE	3-1-0
CSIS125	Blockchain Fundamentals and Use Cases	3-0-2
	Core Elective 3 and 4	
CSIS112	Machine Learning for Security	3-0-2
CSIS118	Software Security	3-0-2
CSIS120	Security and Privacy in the Resource Constrained Environments	3-0-2
CSIS122	Security and Privacy in Social Networks	3-0-2
CSIS126	Adversarial Machine Learning	3-0-2
CSIS128	Mobile Security and Penetration Testing	3-0-2
CSIS130	Secure Software Engineering	3-0-2
CSIS132	Foundations of Privacy Engineering	3-1-0
CSIS134	Bitcoin and Cryptocurrency Technologies	3-0-2
CSIS136	Advanced Cryptography	3-0-2
CSIS138	Security Protocols	3-0-2
CSIS140	Hardware Security	3-0-2
	Institute Elective	
CSIS172	Social Networks	3-0-0
CSIS174	Cyber Laws	3-0-0
CSIS176	Ethical Hacking and Penetration Testing	3-0-2

M. Tech. – I (CSE) ISP Semester – I	L	T	P	C
CSIS101: MATHEMATICAL FOUNDATIONS OF INFORMATION SECURITY (CORE -1)	3	1	0	4

Course Objective	
1	To define and analyse the fundamental concepts of set theory and functions.
2	To study group theory, its applications in the area of cryptography.
3	To analyse the properties of polynomial arithmetic and perform different arithmetic operations.
4	To enable the student to apply the knowledge of abstract algebra in modern cryptosystems.
5	To write rigorous proofs of mathematical results and enhances problem solving skill.

PRELIMINARIES	**(07 Hours)**
Sets, functions, equivalence relations and partitions, mathematical induction.	
GROUPS	**(09 Hours)**
Elementary properties, subgroups, cosets, Lagrange's theorem, Euler's theorem, Fermat's theorem, normal groups, quotient groups, cyclic groups, finite cyclic groups and their properties, homomorphism and isomorphism, Isomorphism theorem, permutation groups, Sylow's theorem and application.	
RINGS AND FIELDS	**(09 Hours)**
Rings, units and zero divisors. Ideals and quotients, principal ideals, prime ideals, maximal ideals, integral domain, PID, Euclidean domain, UFD, Euclidean algorithm for GCD, extended Euclidean algorithm, finding modular inverse of an integer, Chinese RemainderTheorem (CRT), Euler's Phi-function, quadratic residues, fields and field extensions, algebraic extensions, splitting fields.	
FINITE FIELDS	**(10 Hours)**
Construction and examples finite fields, Prime Fields, Binary Extension Field, Arithmetic Operations in Prime Field, Arithmetic Operations in Binary Extension Field, Characterization of finite fields	
POLYNOMIALS	**(10 Hours)**
Roots of irreducible polynomials, Traces, Norms and Bases, Roots of Unity and Cyclotomic polynomials, Order of polynomials and Primitive Polynomials, Irreducible polynomials, Construction of Irreducible polynomials.	
Tutorial Assignments will be based on the coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(15 Hours)**
	(Total Contact Time: 45 Hours + 15 Hours = 60 Hours)

BOOKS RECOMMENDED

1. J. B. Fraleigh, "First Course in Abstract Algebra", Narosa/Addison-Wesley, New Delhi.
2. I N Herstein, "Topics in Algebra, Vikas Publications", New Delhi.
3. R. Lidl and H. Niederreiter, "Introduction to Finite Fields and their Applications", Cambridge University Press, London.
4. David S. Dummit and Richard M. Foote, "Abstract Algebra", 3rd Edition, Wiley.
5. Singh, Y. N, "Mathematical Foundation of Computer Science. India" New Age International (P) Limited Publishers, 2005.

Course Outcomes At the end of the course, students will be able to	
CO1	differentiate among groups, rings and finite fields.

CO2	analyze the algebraic properties of groups, rings and finite fields.
CO3	apply the fundamentals to design and analyze modern day cryptosystems.
CO4	check if a given polynomial is irreducible over a finite field.
CO5	prove essential formal mathematical properties.

M. Tech. – I (CSE) ISP Semester – I	L	T	P	C
CSIS103: DESIGN AND ANALYSIS OF ALGORITHMS (CORE -2)	3	0	2	4

Course Objective	
1	To understand paradigms and approaches used to analyse and design algorithms and to appreciate the impact of algorithm design in practice.
2	To analyse the worst-case time complexity of an algorithm, asymptotic complexities of different algorithms.
3	To design and prove the correctness of the algorithms using appropriate design technique to solve a given real-world computational problem.
4	To analyse and prove the computational intractability of the algorithms of the hard computational problems.
5	To design sub-optimal solutions for the intractable computational problems using alternate design approaches.

INTRODUCTION	**(02 Hours)**
Review of Basis concepts in Algorithms, Abstract Machines, Analysis Techniques: Mathematical, Empirical and Asymptotic analysis, Review of the notations in asymptotic analysis, Recurrence Relations and Solving Recurrences, Proof Techniques – Illustrations	
DIVIDE AND CONQUER APPROACH	**(06 Hours)**
Review of Sorting & order statistics. Various Comparison based Sorts. Analysis. Medians and Order Statistics. The Union-Find problem, Counting Inversions - Finding the closest pair of points. Lower Bound on Sorting and Non-comparison based sorts.	
SEARCHING AN DSET MANIPULATION	**(02 Hours)**
Searching in static table binary search, path lengths in binary trees and applications. Optimality of binary search in worst cast and average-case. Binary search trees, construction of optimal weighted binary search trees. Searching in dynamic table, randomly grown binary search trees, AVL and (a, b) trees.	
HASHING	**(02 Hours)**
Basic ingredients, analysis of hashing with chaining and with open addressing. Union-Find problem: Tree representation of a set, weighted union and path compression-analysis and applications.	
GREEDY DESIGN TECHNIQUE	**(06 Hours)**
Review of Basic Greedy Control Abstraction, Activity Selection Problem & variants, Huffman Coding, Horn Formulas. The Knapsack Problem - Clustering; Minimum-Cost Arborescence. Multi-phase Greedy algorithms. Graph Algorithms. Graph problems: Graph searching. BFS, DFS, shortest first search Minimum Spanning Trees - Single Source Shortest Paths - Maximum Bipartite Cover Problem – Applications., topological sort; connected and bi-connected components. Johnson's implementation of Prim's algorithm using priority queue data structures.	
DYNAMIC PROGRAMMING	**(08 Hours)**
The Coin Changing problem – The Longest Common Subsequence - The 0/1 Knapsack problem, Memoization, Dynamic Programming over Intervals - Shortest Paths and Distance Vector Protocols, Constructing Optimal Binary Search Trees, Algebraic problems: Evaluation of polynomials with or without preprocessing, Winograd's and Strassen's matrix multiplication algorithms and applications to related problems, FFT, simple lower bound results.	
STRING PROCESSING	**(02 Hours)**

String searching and Pattern matching, Knuth-Morris-Pratt algorithm and its analysis, Probabilistic Algorithms.	
BACKTRACKING AND BRANCH & BOUND	**(04 Hours)**
Backtracking, General method, 8-queens problem, Sum of subsets problem, Graph coloring, Hamiltonian cycles. Branch and Bound to solve combinatorial optimization problems	
NP Theory	**(08 hours)**
Polynomial time verification - NP-completeness & the Search Problems - The reductions - Dealing with NP-completeness - Local Search Heuristics – Space complexity. Selected topics - Algorithms for String Matching - Amortized Analysis - Bloom Filters & their applications	
PROBABILISTIC ALGORITHMS	**(02 Hours)**
Indicator Random Variables - Four main design categories - Randomization of deterministic algorithms - Monte Carlo Algorithms - Las Vegas Algorithms - Numerical Probabilistic Algorithms & Various candidate applications therein.	
APPROXIMATION ALGORITHMS	**(03 Hours)**
Introduction and Motivation for Approximation Algorithms – Greedy and combinatorial methods. Scheduling: multiprocessor scheduling.	
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

List of Practical	
1	Lab assignments based on designing algorithms for trivial computational problems and doing their empirical timing analysis.
2	Lab assignments based on designing algorithms using divide and conquer technique and doing their empirical timing analysis.
3	Lab assignments based on designing algorithms using greedy technique and doing their empirical timing analysis.
4	Lab assignments based on designing algorithms using dynamic programming and doing their empirical timing analysis.
5	Lab assignments based on backtracking & branch bound approach to design algorithms.
6	Lab assignments based on designing Approximation algorithms to solve the hard computational problems.

BOOKS RECOMMENDED

1. Cormen, Leiserson, Rivest, Stein, " Introduction to Algorithms", the MIT Press.
2. Knuth, Donald E.: "The Art of Computer Programming, Vol I &III", Pearson Education.
3. Sara Baase , Allen van Gelder , "Computer Algorithms" , Pearson Education.
4. Ellis Horowitz, Sartaj Sahni, "Data Structures, Algorithms and Applications in C++", Universities Press/Orient Longman.
5. J. Kleinberg, E. Tardos: "Algorithm Design", Pearson Education.

ADDITIONAL BOOKS RECOMMENDED

1. K. Mehlhom, "Data Structures and Algorithms, Vol. 1 and Vol. 2", Springer-Verlag, Berlin.
2. A. Borodin and I. Munro, "The Computational Complexity of Algebraic and Numeric Problems", American Elsevier, New York.
3. D. E. Knuth, "The Art of Computer Programming, Vol. 1, Vol. 2 and Vol. 3", Narosa/AddisonWesley, New Delhi/London.
4. Winograd, "The Arithmetic Complexity of Computation", SIAM, New York.

Course Outcomes **At the end of the course, students will**	
CO1	have knowledge about the application of mathematical formula/technique to solve the computational problem.
CO2	be able to understand, identify and apply the most appropriate algorithm design technique required to solve a given problem
CO3	be able to analyze and compare the asymptotic time and space complexities of algorithms.
CO4	be able to write rigorous correctness proofs or implementation for algorithms.
CO5	be able to design and give the solution using innovate/synthesize algorithms to solve the computational problems.

M. Tech. – I (CSE) ISP Semester – I	L	T	P	C
CSIS105: Principles of Information Security and Privacy (CORE -3)	3	0	2	4

Course Objective	
1	To understand the basic principles of Information Security & Privacy management.
2	To understand the basic concepts of the technical components involved in implementing security & privacy.
3	To understand that ensuring information security & privacy in a modern organization is a problem for the management to solve and not one that the technology alone can address.
4	To analyze the important economic and commercial consequences of devising security and privacy solutions in an enterprise or the lack thereof.

INTRODUCTION	**(04 Hours)**
Introduction to Information Security and Privacy: Review of the essential terminologies, basic concepts of security and privacy. Relation or lack thereof between the Information Security, Network Security, Systems Security and the Cyber Security. Key principles of Information Security in terms of Security mechanisms, security attributes and the security attacks. Role of National Security Systems (CNSS) and CERTIN. The McCumber Cube for Security. Introduction to the Security Systems Development Life Cycle and the difference between the Software Security and the Security Software. Classical Security Models.	
SECURITY THREATS AND SECURITY ATTACKS	**(03 Hours)**
Taxonomy of Security attacks. Illustrations of typical attacks. Cyber security threats. The basic terminologies viz. threats, defects, vulnerabilities, exploits, attacks, bugs.	
INTRODUCTION TO INFORMATION PRIVACY	**(05 Hours)**
The importance of Data privacy; Privacy rules; Data Protection – Organization Roles. Approaches to protect sensitive data. Personally Identifiable Information and Sensitive Data. Data Privacy And Protection Responsibilities. Consequences Of Privacy Unawareness. Overview Of Global Data Privacy Laws. The DSCI Privacy Framework for global privacy best practices and frameworks.	
SECURITY TECHNOLOGY – I	**(06 Hours)**
Security Mechanisms: The Symmetric and Asymmetric Key Cryptography, Ciphers: Cryptographic Algorithms and the Cryptosystems, Mechanisms for Data Integrity and Entity Authentication, Access Control mechanisms.	
SECURITY TECHNOLOGY – II	**(06 Hours)**
Cryptographic Tools: The Public-Key-Infrastructure (PKI), Digital Signatures, Digital Certificates, Hybrid Cryptographic Systems, Steganography. The Public Key Cryptography (PKC) limitations and looking beyond the PKC.	
SECURITY TECHNOLOGY – III	**(06 Hours)**
Protocols for Secure Communications: S-HTTP, TLS for Secure Internet Communication, S/MIME, PEM, PGP for Secure Email, the SET, TLS, and S-HTTP for Securing Web Transactions, WEP and WPA for Secure Wireless Communications, Securing TCP/IP with IPSec PGP.	
SECURITY TECHNOLOGY – IV	**(06 Hours)**
Firewalls: Processing Modes, Categorized by Generations, by Structure, Architectures, Selecting the right firewall, Configuring and Managing Firewalls. Remote Access, the concept of Virtual Private Networks.	
SECURITY TECHNOLOGY – V	**(06 Hours)**

Intrusion Detection and Prevention Systems: Why use IDPSs, Types, IDPSs Detection Methods, IDPS Response Behaviour, IDPS Approaches. Strengths and Limitations. Deployment and Implementation of IDPSs. Measuring the effectiveness of IDPSs. Honeypots, Honeynets and Padded Cell Systems. Network Reconnaissance: Network Scanning and Analysis.	
OTHER TOPICS	**(03 Hours)**
Legal and Ethical Issues in Information Security and Privacy. Introduction to Cyber Laws. Introduction to Security policies and Security Acts.	
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

BOOKS RECOMMENDED

1. Michael E. Whitman, Herbert J. Mattord, “Principles of Information Security”, Course Technology Press, 4th edition, 2011.
2. Dieter Gollmann, “Computer Security”, Wiley, 3rd edition, 2014.
3. Gurpreet Dhillon, John Wiley & Sons, “Principles of Information Systems Security: Texts and Cases”, 1st edition, 2006.
4. Andy Taylor, David Alexander, Amanda Finch, David Sutton, “Information Security Management Principles”, 3rd edition, BCS, The Chartered Institute for IT Publishers, 2020.
5. David Sutton, “Cyber Security: A practitioner's guide”, BCS, The Chartered Institute for IT Publishers, 2017.

Course Outcomes
At the end of the course, students will be able to

CO1	Examine and apply the fundamental techniques of computer security.
CO2	Examine and apply and identify potential security issues and the associated risks.
CO3	Demonstrate responsible computer use as it deals with social, political, legal and ethical issues in today's electronic society.
CO4	Demonstrate foundation knowledge of information security/assurance within the organization.
CO5	Plan for the future and design a solution based on user requirements. Explain business continuity, backup and disaster recovery. Understand troubleshooting and quality consumer support.

M. Tech. – I (CSE) ISP Semester – II	L	T	P	C
CSIS102: INFORMATION THEORY AND CODING (CORE – 4)	3	1	0	4

Course Objective	
1	to introduce the principles and applications of information theory.
2	to study about the channel and its capacity, information measure, entropy and coding methods.
3	to teach robust coding schemes and error detection & correcting codes.
4	to learn the concepts of distortion rate, channel capacity and types of channels.
5	to enable the students to design the communication system using efficient coding techniques.

INTRODUCTION	**(05 Hours)**
Information Source, Symbols, and Entropy, Mutual information, information Measures for Continuous Random Variable, Joint and Conditional Entropy, Relative Entropy, Applications Based on information Theoretic Approach.	
SOURCE CODING	**(08 Hours)**
Source Coding Theorem, Kraft inequality, Shannon-Fano Codes, Huffman Codes, Run Length Code, Arithmetic Codes, Lempel-Ziv-Welch Algorithm, Universal Source Codes, Prefix Codes, Variable Length Codes, Uniquely Decodable Codes, instantaneous Codes, Shannon's Theorem, Shannon Fano Encoding Algorithm, Shannon's Noiseless Coding Theorem, Shannon's Noisy Coding Theorem.	
COMMUNICATION CHANNEL	**(08 Hours)**
Channel and its Capacity, Continuous and Gaussian Channels, Discrete Memory-Less Channels, Symmetric Channel, Binary Erasure Channel, Estimation of Channel Capacity, Noiseless Channel, Channel Efficiency, Shannon's Theorem on Channel Capacity, Mimo Channels, Channel Capacity with Feedback.	
VIDEO AND SPEECH CODING	**(07 Hours)**
Video Coding Basics, Quantization, Symbol Encoding, Intraframe Coding, Predictive Coding, Transform Coding, Subband Coding, Vector Quantization, Interframe Coding, Motion Compensated Coding, Image Compression, Jpeg, LZ78 Compression, Dictionary Based Compression, Statistical Modelling, Speech Coding, Psycho-Acousting Modelling, Time Frequency Mapping Quantization, Variable Length Coding, Multichannel Correlation and Irrelevancy, Long Term Correlation, Pre-Echo Control, Bit Allocation.	
ERROR CONTROL CODING	**(12 Hours)**
Overview of Field, Group, Galois Field, Types of Codes, Hamming Weight, Minimum Distance Based Codes, Error Detection and Error Correction Theorems, Maximum Likelihood Decoder, Map Decoder, Linear Block Codes and Their Properties, Equivalent Codes, Generator Matrix and Parity Check Matrix, Systematic Codes, Cyclic Codes, Convolution Codes and Viterbi Decoding Algorithm, Iterative Decoding, Turbo Codes and Low Density-Parity-Check Codes, Asymptotic Equipartition Property, Bch Codes, Generator Polynomials, Decoding of Bch Codes, Reed Solomon Codes, Trellis Codes, Space Time Coding.	
RATE DISTORTION THEORY	**(05 Hours)**
Rate Distortion Function, Random Source Codes, Joint Source-Channel Coding and the Separation Theorem.	
Tutorial Assignments will be based on the coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(15 Hours)**

(Total Contact Time: 45 Hours + 15 Hours = 60 Hours)

BOOKS RECOMMENDED	
1.	R. Bose, "Information Theory, Coding and Cryptography", McGraw-Hill, 3rd Ed., 2016.
2.	T. M. Cover and J. A. Thomas," Elements of information Theory", John Wiley & Sons, New York, 2012.
3.	A. B. Robert, "Information Theory", Dover Special Priced Titles, 2007.
4.	R. M. Roth, "Introduction to Coding Theory", Cambridge University Press, 2006.
5.	Reza, "An introduction to information Theory", Dover, 1994.

Course Outcomes At the end of the course, students will	
CO1	have knowledge about the importance of coding techniques in communication systems and different methods for the same.
CO2	be able to apply information theory concepts and linear algebra in source coding and channel coding.
CO3	be able to analyze the performance of different channel coding techniques using different error control techniques.
CO4	be able to evaluate different types of channels using different coding techniques using statistical techniques.
CO5	be able to design and innovate a solution using the knowledge of coding techniques and rate distortion theory for different types of communication channels.

M. Tech. – I (CSE) ISP Semester – II	L	T	P	C
CSIS104: NETWORK SECURITY (CORE - 5)	3	0	2	4

Course Objective	
1	To understand basics of network security, computer and network security threats and basic paradigms and approaches used in network security at various layers.
2	To analyze existing authentication and key agreement protocols and to identify weaknesses of these protocols.
3	To acquire knowledge on standard algorithms used to provide confidentiality, integrity and authenticity.
4	To develop basic skills of secure network architecture and addressing network security issues, challenges and mechanisms.
5	To develop various security solutions against real life security threats.

INTRODUCTION	**(08 Hours)**
Model for Network Security, Network Security Threats, Attacks and Countermeasures, Importance of Effective Network Security Strategies, Overview of Cryptographic Primitives	
SECURITY AT THE APPLICATION LAYER	**(08 Hours)**
S/MIME-Functionality, Messages and Certificate Processing, Domain Keys Identified Mail, Pretty Good Privacy (PGP), GNU Privacy Guard (GPG)	
SECURITY AT THE TRANSPORT LAYER	**(07 Hours)**
SSL/TLS Architecture, Handshake Protocol, Change Cipher Spec Protocol, Alert Protocol, Record Protocol, SSL Message formats, Https, Secure Shell (SSH).	
SECURITY AT THE NETWORK LAYER	**(07 Hours)**
IP Security Overview, IP Security Policy, Encapsulating Security Payload, internet Key Exchange, Authentication Header.	
WIRELESS NETWORK SECURITY	**(07 Hours)**
Wireless Security, Mobile Device Security, IEEE 802.11i Wireless LAN Security, WEP and WPA Protocols.	
NETWORK ACCESS CONTROL AND CLOUD SECURITY	**(08 Hours)**
Network Access Control, Extensible Authentication Protocol, IEEE 802.1x Port-Based Network Access Control, Cloud Computing, Cloud Security Risks and Countermeasures, Data Protection in the Cloud, Cloud Security as a Service, Addressing Cloud Computing Security Concerns.	

Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

BOOKS RECOMMENDED

1. William Stallings, “Network Security Essentials: Applications and Standards”, Fourth Edition, 2011.
2. Charlie Kaufman, Radia Perlman, Mike Speciner, “Network Security: Private Communication in a Public World”, 2nd Ed., Prentice Hall PT, 2002.
3. William Stallings, “Cryptography and Network Security: Principles and Practice”, 7th Ed. Pearson, 2017.

4. Behrouz forouzan, Debdeep Mukhopadhyay, "Cryptography and Network Security", 2nd Ed., Tata McGraw-Hill Education. 2010.
5. Chris McNab, "Network Security Assessment". 3rd Ed., O'Reilly Media, 2004.

Course Outcomes **At the end of the course, students will**	
CO1	be able to assess vulnerability and weaknesses in the network.
CO2	be able to understand network security techniques to protect against threats in the network.
CO3	be able to analyze different network security techniques to identify, classify the network security threats and select suitable for the given application scenario.
CO4	be able to set up firewall and intrusion detection system for organization's security and evaluate possible threats and attacks at various layers of TCP/IP suite.
CO5	be able to design robust and efficient system for network security for organizations.

M. Tech. – I (CSE) ISP Semester – I	L	T	P	C
CSIS111: MODERN CRYPTOGRAPHY (CORE ELECTIVE-1 OR 2)	3	1	0	4

Course Objective	
1	to understand group theory, number theory, and discrete probability.
2	to analyze probabilistic algorithms.
3	to develop the ability to model security problems and to write security proofs.
4	to understand fundamental cryptographic primitives including Key Exchange, Digital Signatures, Oblivious Transfer, Public-Key Encryption, Commitment.
5	to understand basic computational problems that are important for cryptography such factoring problem, the RSA problem, the discrete-logarithm problem.

INTRODUCTION	**(04 Hours)**
Classical Cryptography and Modern Cryptography, Principles of Modern Cryptography, formal Definitions, Precise Assumptions, Proofs of Security, Provable Security and Real-World Security	
PERFECTLY SECRET ENCRYPTION	**(04 Hours)**
Formal Definitions, Shannon's Theory, one-Time Pad, Limitations of Perfect Secrecy.	
PRIVATE-KEY ENCRYPTION	**(06 Hours)**
Defining Computationally Secure Encryption, Semantic Security, Constructing Secure Encryption Schemes-Pseudorandom Generators and Stream Ciphers, Proofs by Reduction, Cryptanalytic Attacks-Chosen-Plaintext Attacks and CPA-Security, Constructing CPA-Secure Encryption Schemes, Pseudorandom Functions and Block Ciphers, Cpa-Secure Encryption From Pseudorandom Functions, Chosen-Ciphertext Attacks- Defining CCA-Security.	
HASH FUNCTIONS AND APPLICATIONS	**(05 Hours)**
Hash Functions-one-Wayness and Collision Resistance, Merkle–Damgard Construction, Attacks on Hash Functions-Birthday Attacks, Random-oracle Model, Merkle Trees.	
MESSAGE AUTHENTICATION CODES	**(06 Hours)**
Message Authentication Codes – formal Definitions, Design, and Proof of Security, HMAC, CBC-MAC, Authenticated Encryption, information-Theoretic Macs, Limitations on information-Theoretic Macs	
ALGORITHMS FOR FACTORING AND COMPUTING DISCRETE LOGARITHMS	**(06 Hours)**
Algorithms for Factoring-Pollard's P − 1 Algorithm, Pollard's Rho Algorithm , Quadratic Sieve Algorithm, Algorithms for Computing Discrete Logarithms- Pohlig–Hellman Algorithm, Baby-Step/Giant-Step Algorithm, Discrete Logarithms From Collisions, index Calculus Algorithm.	
PUBLIC-KEY ENCRYPTION	**(06 Hours)**
RSA Encryption, Security Against Chosen-Plaintext Attacks, Security Against Chosen-Ciphertext Attacks, RSA Implementation Issues and Pitfalls, Computational Diffie-Hellman/Decisional Diffie-Hellman Based Encryption, Elliptic Curve Cryptography-Elliptic Curve Over Finite Fields and Binary Fields, Point Addition Operation, Elliptic Curve Discrete Logarithm Problem, Cryptosystems Based on Elliptic Curve.	
ADVANCED TOPICS	**(08 Hours)**
Zero-Knowledge Proofs, Secret Sharing Schemes, Lattices and Cryptography	
Tutorial Assignments will be based on the coverage of above topics.	**(15 Hours)**
(Total Contact Time: 45 Hours + 15 Hours = 60 Hours)	

BOOKS RECOMMENDED

1. Katz & Lindell, “Introduction to Modern Cryptography: Principles and Protocols”, Second Edition, Publisher: Chapman & Hall/CRC, 2014.
2. Douglas R. Stinson, “ Cryptography: Theory and Practice”, Third Edition, Publisher: Chapman and Hall/CRC, 2005.
3. Goldreich, “Foundations of Cryptography”, Cambridge University Press, 2005 (Volume 1 and 2).
4. William Stallings, “Cryptography and Network Security: Principles and Practice”, 7th Ed. Pearson, 2017.
5. Katz, Jonathan, and Lindell, Yehuda, “ Introduction to Modern Cryptography”. United States, CRC Press, 2020.

Course Outcomes **At the end of the course, students will**	
CO1	communicate formal security definitions, security assumptions and security proofs of modern cryptosystems.
CO2	differentiate various deterministic and probabilistic algorithms and understand their applicability in real-world application scenarios.
CO3	present the security models and security proofs of well-known algorithms.
CO4	demonstrate familiarity with fundamental cryptographic primitives and apply the knowledge to various application domains.
CO5	compare number theoretic problems used by cryptographic algorithms and evaluate their respective strengths and weaknesses.

M. Tech. – I (CSE) ISP Semester – I	L	T	P	C
CSIS113: CLOUD COMPUTING AND BIG DATA ANALYTICS (CORE ELECTIVE-1 OR 2)	**3**	**0**	**2**	**4**

Course Objective	
1	To understand the cloud computing and Big data platform and its use cases.
2	To identify the techniques achieving cloud based big data analytics with scalability and streaming capability.
3	To apply different algorithms and techniques of big data analytics using appropriate cloud platforms to solve complex problems.
4	To analyse and evaluate suitable cloud paradigms and big data analytics algorithms and techniques to give solutions for complex problems.
5	To design and give solutions for given problems through big data analytics tools and cloud platform.

INTRODUCTION	**(09 Hours)**
History and introduction of Cloud Computing, Big Data Analytics, Data Warehousing, Data Mining	
CLOUD COMPUTING	**(09 Hours)**
Virtualization, SOA, Programming Model, Resource Management and Scheduling, Application building for Managing and Analyzing Data	
BIG DATA ANALYTICS	**(09 Hours)**
Concepts and Techniques in Data Warehousing, Concept Description and Association Rule Mining, Classification and Prediction, Hadoop Map-Reduce Platforms, Stream Computing Platforms and Algorithms	
NOSQL DATABASES AND SCALABLE DATA STORAGE	**(09 Hours)**
Graph databases, Mongo and Cassandra	
ADVANCED TOPICS	**(09 Hours)**
Structured and high dimensional data, Real time stream analytics, Generalized functional decomposition, Apache Spark and Storm	
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

BOOKS RECOMMENDED

1. J. Leskovec, A. Rajaraman, J. D. Ullman, “Mining of Massive Datasets”, Cambridge
2. White, Tom, “Hadoop: The Definitive Guide”, United States, O'Reilly Media, 2012.
3. M. Parsian, “Data algorithms: Recipes for scaling up with Hadoop and Spark”
4. K. Hwang, M. Chen, “Big-Data Analytics for Cloud, IoT and Cognitive Computing”, Willey
5. Nikos Antonopoulos, Lee Gillam, "Cloud Computing: Principles, Systems and Applications", Springer.

ADDITIONAL BOOKS RECOMMENDED

1. Rajkumar Buyya, James Broberg, Andrzej M. Goscinski: "Cloud Computing: Principles and Paradigms", Wiley

Course Outcomes **At the end of the course, students will**	
CO1	have the knowledge of concepts, technologies, architecture and applications cloud computing and big data analytics.
CO2	be able to identify techniques achieving cloud based big data analytics with scalability and streaming capability.
CO3	be able to apply different algorithms and techniques of big data analytics using appropriate cloud platforms to solve complex problems.
CO4	be able to analyse and evaluate suitable cloud paradigm and big data analytics algorithms and techniques to give solutions for complex problems.
CO5	be able to design and give solutions for given problems through big data analytics tools and cloud platforms.

M. Tech. – I (CSE) ISP Semester – I	L	T	P	C
CSIS115: MACHINE LEARNING (CORE ELECTIVE-1 OR 2)	3	0	2	4

Course Objective	
1	to understand the basic concepts, state-of-the art techniques of machine learning, statistical analysis and discriminant functions
2	to study various supervised, unsupervised learning algorithms, classification, clustering, neural networks and different types of neural networks
3	to apply and analyze dimensionality reduction techniques
4	to understand and evaluate kernel methods to use them in various non-parametric approaches
5	to design an algorithm or optimum solution using different machine learning approaches

INTRODUCTION	(09 Hours)
Pattern Representation, Concept of Pattern Recognition and Classification, Feature Extraction, Feature Selection, Basics of Probability, Bayes Decision Theory, Maximum-Likelihood and Bayesian Parameter Estimation, Error Probabilities, Learning of Patterns, Modelling, Regression, Discriminant Functions, Linear Discriminant Functions, Decision Surface, Learning Theory, Fisher Discriminant Analysis.	
SUPERVISED LEARNING ALGORITHMS	**(09 Hours)**
Linear Regression, Gradient Descent, Support Vector Machines, Artificial Neural, Networks, Decision Trees, Ml and Map Estimates, K-Nearest Neighbor, Naïve Bayes, Bayesian Networks, Classification, Overfitting, Regularization, Multilayer Networks, Back-Propagation, Bayes Classification, Nearest Neighbor Classification, Cross Validation and Attribute Selection, K Means Clustering, Agglomerative Hierarchical Clustering, Deep Neural Networks, Convolutional Neural Networks, Recurrent Neural Networks.	
UNSUPERVISED LEARNING ALGORITHMS	**(09 Hours)**
K-Means Clustering, Gaussian Mixture Models, Learning with Partially Observable Data, Expectation Maximization Approach. Dimensionality Reduction, Principal Component Analysis, Model Selection and Feature Selection, Regularization, Theory of Generalization: in-Sample and Out-of-Sample Error, VCinequality, VC Analysis.	
NON PARAMETRIC APPROACH	**(08 Hours)**
Kernel Methods, Basic Kernels, Types of Kernel, Properties of Kernels, Pattern Analysis Using Eigen Decomposition, Principal Component Analysis, Hidden Markov Models, Markov Decision Processes, Non-parametric Techniques for Density Estimation, Parzen-Window Method.	
APPLICATIONS	**(10 Hours)**
Signal Processing Application, Image Processing, Biometric Recognition, Face and Speech Recognition, information Retrieval, Natural Language Processing.	
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

BOOKS RECOMMENDED

1. Richard O. Duda, Peter E. Hart, David G. Stork, “Pattern Classification”, 2nd Ed., Wiley, 2001.
2. Christopher M. Bishop, “Pattern Recognition and Machine Learning”, Springer, 2006.
3. Geoff Dougherty, “Pattern recognition and classification an introduction”, Springer, 2013.
4. Richard O. Duda and Peter E. Hart, “Pattern Classification and Scene Analysis”, John Wiley &

Sons, 1973.
5. John Shae Taylorand Nello Cristianini, “Kenerl methods for patten analysis” Cambaridge university press, 2004.

ADDITIONAL BOOKS RECOMMENDED

1. Ranjjan Shinghal, “Pattern Recognition techniques and application”, Oxford university press, 2006.
2. Theodoridis and K.Koutroumbas, “Pattern Recognition”, 4th Ed., Academic Press, 2009.

Course Outcomes **At the end of the course, students will**	
CO1	have knowledge of pattern recognition, regression, classification, clustering algorithms and statistics.
CO2	be able to apply different feature extraction, classification, regression, neural network algorithms and modeling.
CO3	be able to analyze the data patterns and modeling for applying the learning algorithms and non-parametric approaches.
CO4	be able to evaluate the performance of an algorithm and comparison of different learning techniques.
CO5	be able to design solution for real life problems like biometric recognition, natural language processing and its related applications using various tools and techniques of machine learning.

M.Tech-I Semester – I	L	T	P	C
CSIS117: CYBER PHYSICAL SYSTEMS (CORE ELECTIVE-1 OR 2)	3	0	2	4

Course Objective:	
1	To have an understanding of the cyber physical systems and the corresponding important research challenges in this area.
2	To be able to learn the evolution in computing from mainframe computing to the ubiquitous and pervasive computing and the dominant role of the embedded systems.
3	To be able to understand various modelling formalisms for the CPSs, viz. Timed and Hybrid Automata and do the formal analysis using flow pipe construction, reachability analysis of CPS Software.
4	To be able to analyze and design the protocols used in resource constrained environments.
5	To be able to improve the critical reading, presentation, and research skills.

INTRODUCTION	**(04 Hours)**
Introduction to Cyber-Physical Systems. The Industrial Revolution 4.0. Motivation for the IR 4.0. Cyber-Physical Systems (CPS) in the real world.	
WIRELESS SENSOR NETWORK AND INTERNET OF THINGS	**(10 Hours)**
Basic principles of design and validation of CPS. Basic characteristics of the CPSs. The Internet of Things. The Industrial Internet of Things. The Wireless Sensor Networks and the RFID devices as the actors of the CPSs. The Ubiquitous and the Pervasive Computing paradigm introduced by the CPSs. The Applications of the Wireless Sensor Networks. The role of the Internet of Things in realizing Smart Applications. The Characteristics and the issues of deployment.	
CPS HARDWARE	**(09 Hours)**
CPS Hardware Platforms: Processors. Types of Processor. The Processors Design issues. Parallelism. Embedded Processors. Harvard Architecture: Pros and Cons. The Sensors and Actuators. Models of Sensors and Actuators. Common Sensors. Actuators. Memory Architectures. Memory Technologies. Memory Hierarchy. Memory Models. Types of memory in the CPSs. Input and Output Hardware. The design issues. The Analog to Digital convertor.	
CPS OPERATING SYSTEMS AND NETWORKING	**(09 Hours)**
Realtime Operating Systems for the WSN devices. Characteristics. Issues. Thread Scheduling. Basics of Scheduling. Rate Monotonic Scheduling. The Earliest Deadline First Scheduling. Scheduling and Mutual Exclusion. Multiprocessor Scheduling. Sequential Software in a Concurrent World. Multitasking. Imperative Programs. Case studies of the typical OSs. TinyOS, nesC and Contiki. The Simulators for the WSN devices. The CPS Network - WirelessHart, CAN, Automotive Ethernet.	
CPS MODELLING AND ANALYSIS	**(09 Hours)**
Formal Methods for Safety Assurance of Cyber-Physical Systems: Advanced Automata based modelling and analysis, Basic introduction and examples, Timed and Hybrid Automata, Definition of trajectories, Formal Analysis: Flow pipe construction, reachability analysis. Analysis of CPS Software: Weakest Preconditions, Bounded Model checking, CPS software verification: Frama-C, CBMC	
CPS SECURITY	**(04 Hours)**
Secure Deployment of CPS: Attack models, Secure Task mapping and Partitioning, State estimation for attack detection Automotive Case study: Vehicle ABS hacking Power Distribution Case study: Attacks on SmartGrids.	
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

BOOKS RECOMMENDED

1. E. A. Lee and S. A. Seshia , " Introduction to Embedded Systems - A Cyber-Physical Systems Approach", Second Edition, The MIT Press, 2017.
2. Rajeev Alur,"Principles of Cyber-Physical Systems", The MIT Press. 2015
3. ZEADALLY S and Nafaâ Jabeur, "Cyber Physical System Design with Senor Networking Technologies, The IET Press. 2016.
4. Taha, W. M., Taha, A. M., Thunberg, J.,"Cyber-Physical Systems: A Model-Based Approach", Germany: Springer International Publishing, 2020
5. Rajkumar, R., de Niz, D., Klein, M, "Cyber-Physical Systems". United Kingdom: Pearson Education, 2016.

Course Outcomes **At the end of the course, students will be able to**	
CO1	Understand the fundamentals of cyber-physical systems (CPS).
CO2	Apply the concepts of CPS to the different paradigms of computing.
CO3	Analyze the design issues associated with different hardware functional units of the CPSs.
CO4	Evaluate the performance impact of thread scheduling algorithms in the CPSs.
CO5	Design CPS solutions for different application domains.

M. Tech. – I (CSE) ISP Semester – I	L	T	P	C
CSIS119: DIGITAL FORENSICS (CORE ELECTIVE-1 OR 2)	3	0	2	4

Course Objective	
1	To understand the basics of digital forensics and different cyber-crimes.
2	To identify the need of digital forensic and the role of digital evidence used to investigate the cyber-crime.
3	To understand the system activity logs to perform the scripting for investigating cyber-crime.
4	To investigate digital evidence such as the data acquisition, identification analysis and techniques for conducting the forensic examination on different digital devices.
5	To learn the various tools to perform the operations on data in order to assess the cyber crime

INTRODUCTION	**(06 Hours)**
Introduction to Digital Forensics, Definition and Types of Cybercrimes, Rules for Digital Forensic, Need for Digital Forensics, Types of Digital Forensics, Ethics in Digital Forensics, Introduction to Internet Crimes, Hacking and Cracking, Credit Card and ATM Frauds, Web Technology, Cryptography.	
CYBER CRIME AND DIGITAL EVIDENCES	**(08 Hours)**
Types of Digital Evidences and their Characteristics, Electronic Evidence and Handling, Challenges in Digital Evidence Handling, Searching and Storage of Electronic Media, Emerging Digital Crimes and Modules, Understanding Law Enforcement Agency Investigations, Following the Legal Process, Understanding Corporate Investigations, Establishing Company Policies.	
COMPUTER SECURITY INCIDENT RESPONSE	**(07 Hours)**
Introduction to Computer Security Incident, Goals of Incident Response, Incident Response Methodology, Formulating Response Strategy, Incident Response Process, Data Collection on Unix Based Systems.	
DISK AND FILE SYSTEM ANALYSIS	**(08 Hours)**
Media Analysis Concepts, File System Abstraction Model, Partition Identification and Recovery, Virtual Machine Disk Images, Forensic Containers Hashing, Carving, Forensic Imaging, Data Analysis Methodology, Investigating Applications, Malware Handling.	
IDENTIFICATION OF DATA	**(08 Hours)**
Identification of Data: Timekeeping, Forensic Identification and Analysis of Technical Surveillance Devices, Reconstructing Past Events, Useable File Formats, Unusable File Formats, Converting Files, Investigating Network Intrusions and Cyber Crime, Network Forensics and Investigating Logs, Investigating Network Traffic, Investigating Web Attacks, Router Forensics. Cyber Forensics Tools and Case Studies.	
NETWORK FORENSICS	**(08 Hours)**
Technical Exploits and Password Cracking, Analyzing Network Traffic, Collecting Network Based Evidence, Evidence Handling, Investigating Routers, Handling Router Table Manipulation Incidents, Using Routers As Response Tools.	
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

BOOKS RECOMMENDED

1. Jason Luttgens, Matthew Pepe, Kevin Mandia, "Incident Response and computer forensics", Tata McGraw Hill, 2014.
2. Nilakshi Jain, Dhananjay Kalbande, "Digital Forensic: The fascinating world of Digital Evidences", Wiley, 2016.
3. C. Altheide& H. Carvey, "Digital Forensics with Open Source Tools, Syngress", 2011. ISBN: 9781597495868.
4. Angus M.Marshall, "Digital forensics: Digital evidence in criminal investigation", John – Wiley and Sons, 2008.
5. Amelia Phillips, Bill Nelson, Christopher Steuart, "Guide to Computer Forensics and Investigations", Fourth Edition, Course Technology, 2009.

Course Outcomes **At the end of the course, students will**	
CO1	have the knowledge of various cybercrimes and the concepts of digital forensic, and handling evidence.
CO2	be able to apply appropriate response Strategy and the overall incidence response process.
CO3	be able to analyze the data and handling of malware.
CO4	be able to evaluate different evidence and methodologies for forensic analysis.
CO5	be able to design the digital forensic system to carry out system level forensics for cybercrimes.

M.Tech.I Semester – I	L	T	P	C
CSIS121: DEFENSIBLE SECURITY ARCHITECTURE (CORE ELECTIVE-1 OR 2)	3	0	2	4

Course Objective	
1	To learn the basic principles of traditional network and security architectures and analyse their common weaknesses.
2	To understand the design and architecture of defensible systems and networks.
3	To learn the fundamentals of traditional vs defensible security architectures, security models.
4	To be able to analyze and design an application to follow the defensible security architectures life cycle or DARIOM (Discover, Assess, Re-Design, Implement and Monitor) model.
5	To be able to design the application architecture ensuring that the application performs its operational functions effectively and security complements this goal.
6	To understand the principle of Time-Based Security and how to implement it in real world.

INTRODUCTION	**(10 Hours)**
Introduction: Course Overview, What is a Security Architecture? What makes a good Security Architect? Learning through Case (Tyrell Corp Case Study or any other to be selected). Traditional Security Architecture Deficiencies, Emphasis on Perimeter/Exploitation, Lack of a True Perimeter ("De-perimeterization" as a Result of Cloud/Mobile). The concept of Zero Trust and Defensible Security Architecture Mindset. The Presumption of Compromise De-perimeterization, The limitations of Think Red, Act Blue, approach. Overview of the Security Architectures in The Internet of Things.	
SECURITY MODELS	**(08 Hours)**
Security Models. Time Based Security. Cyber Kill Chain: Intelligence Driven Defense® model for identification and prevention of cyber intrusions. The Zero Trust Model, Zero Trust Architecture. Threat, Vulnerability, and Data Flow Analysis. Defensible Security Architecture Life Cycle (DARIOM Model). Threat Vector Analysis. Attack Surface Analysis. Physical Security Best Practices. Network Security Best Practices. Layer 2 Attacks and Mitigation. NetFlow for IP network traffic analysis. Layer 2 and 3 NetFlow. NetFlow, Sflow, Jflow, VPC Flow, Suricata and Endpoint Flow. Cloud Flows	
NETWORK SECURITY ARCHITECTURE	**(10 Hours)**
Network Security Architecture and Network-centric Applications Security Architecture: Layer 3 Attacks and Mitigation: IP Source Routing, ICMP Attacks, Unauthorized Routing Updates, Securing Routing Protocols, Unauthorized Tunneling (Wormhole Attack). Switch and Router Best Practices: Layer 2 and 3 Benchmarks and Auditing Tools. Baselines. Securing SNMP. Hardening SNMP. Securing NTP. Bogon Filtering, Blackholes, and Darknets. Bogon Filtering. Monitoring Darknet Traffic. Securing IPv6: IPv6 Firewall Support, Scanning IPv6, IPv6 Asset Inventory with Rumble Network Discovery, IPv6 Tunneling, IPv6 Router Advertisement Attacks and Mitigation. Segmentation: Network vs Access Segmentation. Firewall Architecture: DMZ Design, Layer 3/4 Stateful Firewalls, Router ACLs, Linux and BSD Firewalls. Azure Privileged Management (PIM). Application Proxies. SMTP Proxy. Augmenting with Phishing Protection and Detection Mechanisms. Next-Generation Firewall: (NGFW): Application Filtering, Implementation Strategies. Network Security Monitoring (NSM). NIDS/NIPS. Sandboxing. The "Encrypt Everything" Mindset. HSTS Preloading. Certificate Transparency Monitoring. Crypto Suite Support. Distributed Denial-of-Service Protection. Impact of Internet of Things. Types of Attacks. Mitigation Techniques	
DATA-CENTRIC SECURITY ARCHITECTURES	**(08 Hours)**
Data-centric Security architecture. Application (Reverse) Proxies. Full Stack Security Design. Web Application Firewalls. Database Firewalls/Database Activity Monitoring. File Classification Data Discovery. Dynamic Access Control. Data Loss Prevention (DLP): Network-based, Endpoint-based,	

Cloud Application Implementations. Data Governance, Mobile Device Management (MDM) and Mobile Application Management (MAM). Security Policies. Private Cloud Security. Public Cloud Security Challenges. Container Security	
ZERO TRUST ARCHITECTURES	**(09 Hours)**
Zero Trust Architectures: Why Perimeter Security Is Insufficient? What Zero Trust Architecture Means. "Trust but Verify" vs. "Verify then Trust". Credential Rotation. Adaptive Trust and Security Orchestration. Authenticating and Encrypting Endpoint Traffic. Domain Isolation (Making Endpoint Invisible to Unauthorized Parties). Mutual TLS. Segmentation Gateways. Leveraging Endpoints as Hardened Security Sensors. End-user Privilege Reduction. Scaling Endpoint Log Collection/Storage/Analysis: How to Enable Logs that Matter, Designing for Analysis Rather than Log Collection, Auditing Policies on Windows and Linux: Sysmon, Auditd. Tripwire and Red Herring Defenses: Honeynets, Honeypots, and Honeytokens, Single Access Detection Techniques, Proactive Defenses to Change Attacker Tool Behaviors, Increasing Prevention Capabilities while Adding Solid Detection.	
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**
	(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)

BOOKS RECOMMENDED

1. Ed Moyle (Author), Diana Kelley , “Practical Cybersecurity Architecture: A guide to creating and implementing robust designs for cybersecurity architects”, Packt Publishing Limited, 2020.
2. Heather Adkins, Betsy Beyer, Paul Blankinship, Piotr Lewandowski, Ana Opera and Adam Stubblefield , “Building Secure & Reliable Systems: Best Practices for Designing, Implementing and Maintaining Systems”, O’Reilly Shroff Publishers, 2020.
3. Evan Gilman, Doug Barth , “Zero Trust Networks: Building Secure Systems in Untrusted Networks Paperback – 1”, O’Reilly Shroff Publishers, 2017.
4. Chris Dotson ,“Practical Cloud Security: A Guide for Secure Design and Deployment 2019”, O’Reilly Shroff Publishers, 2017.
5. Jason Garbis, Jerry W. Chapman , “Zero Trust Security: An Enterprise Guide Paperback”, Apress Publishers, 1st edition, 2021.

Course Outcomes **At the end of the course, students will able to**	
CO1	Learn the basic principles of traditional network and security architectures.
CO2	Analyse the common weaknesses of the traditional security architectures and understand the significance of the defensible security architectures.
CO3	Build and design models of the defensible systems and networks.
CO4	Analyze and design an application to follow the defensible security architectures life cycle or DARIOM (Discover, Assess, Re-Design, Implement and Monitor) model.
CO5	Design the application architecture ensuring that the application performs its operational functions effectively and security complements this goal.
CO6	Understand the principle of Time-Based Security and how to implement it in real world.

M. Tech. – I (CSE) ISP Semester – I	L	T	P	C
CSIS123: RESEARCH METHODOLOGY IN CSE (CORE ELECTIVE-1 OR 2)	3	1	0	4

Course Objective	
1	To understand the basic terminology of research, its methodology and learn different methodologies of pursuing the research in terms of organization, presentation and evaluation.
2	To apply the concept in writing the technical content.
3	To analyze the existing method using different parameters in different scenarios.
4	To evaluate the proposed work and compare with existing approaches systematically using the appropriate methodology, through simulation depending upon the research field.
5	To design algorithms using concepts learned and write reports and papers technically and grammatically correct.

INTRODUCTION	**(04 Hours)**
Research: Definition, Characteristics, Motivation and Objective, Research Methods vs Methodology, Types of Research – Descriptive vs Analytical, Applied vs Fundamental, Quantitative vs Qualitative, Conceptual vs Empirical.	
METHODOLOGY	**(04 Hours)**
Research Process, Formulating the Research Problem, Defining the Research Problem, Research Questions, Research Methods vs. Research Methodology.	
LITERATURE REVIEW	**(04 Hours)**
Review Concepts and Theories, Identifying and Analyzing the Limitations of Different Approaches.	
FORMULATION AND DESIGN	**(05 Hours)**
Concept and Importance in Research, Features of a Good Research Design, Exploratory Research Design, Concept, Types and Uses, Descriptive Research Designs, Concept, Types and Uses, Experimental Design: Concept of Independent & Dependent Variables.	
DATA MODELING AND SIMULATIONS	**(08 Hours)**
Mathematical Modeling, Experimental Skills, Simulation Skills, Data Analysis and Interpretation.	
TECHNICAL WRITING AND TECHNICAL PRESENTATIONS	**(05 Hours)**
CREATIVITY AND ETHICS IN RESEARCH, INTELLECTUAL PROPERTY RIGHTS	**(05 Hours)**
TOOLS AND TECHNIQUES FOR RESEARCH	**(06 Hours)**
Methods to Search Required Information Effectively, Reference Management Software, Software for Paper Formatting, Software for Detection of Plagiarism.	
DISCUSSION AND DEMONSTRATION OF BEST PRACTICES	**(04 Hours)**
(Total Contact Time: 45 Hours + 15 Hours = 60 Hours)	

BOOKS RECOMMENDED

1. John W. Creswell, “Research Design: Qualitative, Quantitative, and Mixed Methods Approaches”, SAGE Publications Ltd.
2. C.R. Kothari,”Research Methodology: Methods and Techniques”, New Age International Publishers.
3. David Silverman,”Qualitative Research”, SAGE Publications Ltd.
4. Norman K. Denzin and Yvonna Sessions Lincoln,”Handbook of Qualitative Research”, SAGE Publications Ltd.
5. Michael Quinn Patton, ”Qualitative Research and Evaluation Methods”, SAGE Publications Ltd.

Course Outcomes **At the end of the course, students will**	
CO1	have an understanding of the different research methodology in different areas.
CO2	be able to apply the concepts in writing, presentation, and simulating different experiments.
CO3	be able to analyze the proposed work with existing approaches in the literature and interpret the research design through project development and case study analysis using appropriate tools.
CO4	be able to execute the technical presentation, organization in writing the report and papers.
CO5	be able to design the algorithms and proof learned and communicate effectively through proper organization and presentation.

M. Tech. – I (CSE) ISP Semester – II	L	T	P	C
CSIS125: BLOCKCHAIN FUNDAMENTALS AND USE CASES (CORE ELECTIVE-3 OR 4)	**3**	**0**	**2**	**4**

Course Objective	
1	to demonstrate a familiarity with the concepts related to blockchain technology.
2	to apply the knowledge of cryptography and distributed systems to design decentralized applications.
2	to design and build smart contracts and distributed applications (DApps) for different applications.
3	to analyse and explore the real-world applications of blockchain technology.
4	to assess the strengths and weaknesses of blockchain enabled decentralization in different application scenarios.

INTRODUCTION	**(08 Hours)**
Introduction to Blockchain and Digital Currency, Evolution, Blockchain as Public ledger, Structure of a Block, Transactions, Merkel Trees, Peer-to-Peer Networks, Timestamp, Double Spend Problem, Decentralization Applications, Characteristics, Benefits and Challenges.	
CRYPTOGRAPHY IN BLOCKCHAIN	**(08 Hours)**
Hash Functions, Public Key Cryptosystem, Public Key Generation, Digital Signature, Zero-Knowledge Proof, k-Anonymity.	
SMART CONTRACTS AND CONSENSUS ALGORITHMS	**(05 Hours)**
Smart Contract, Applications of Smart Contracts, Mining, Hardness of Mining, Incentive, Consensus, Paxos, Consensus Algorithms - PBFT, PoW, PoS, etc.	
DISTRIBUTED COMPUTING IN BLOCKCHAIN	**(07 Hours)**
Distributed System, Multi-Party Consensus Algorithm, Distributed Denial of Service (DDoS), Secure Multiparty Computation, Byzantine Generals Problem, Byzantine Fault Tolerance based and Leader-based Consensus Mechanism, CAP Theorem, Client-Server Model, Virtual Machines- Ethereum Virtual Machine (EVM) and Tron Virtual Machine (TVM), Quorum Systems, DApps.	
ETHEREUM AND HYPERLEDGER	**(07 Hours)**
Ethereum, Trustlessness and Immutability of Blockchain Technology, Proof of Work (PoW) andProof of Stake (PoS), Ethereum Virtual Machine (EVM), Wallets for Ethereum, Solidity, Hyperledger, Corda, Hyperledger Fabric, Hyperledger Composer, Permissioned vs Permissionless Blockchain.	
BLOCKCHAIN FOR REAL-WORLD APPLICATIONS	**(06 Hours)**
Cryptocurrencies, Banking, Supply Chain, Healthcare, Real-Estate, Judiciary, IoT, Insurance, etc.	
ADVANCED TOPICS	**(04 Hours)**
Pool Mining, Sybil Attacks, Scalability of Blockchain, Smart Contract Vulnerabilities, Finalizing Transaction, Privacy Leakage. Note: topics Will Be Revised Time to Time According to Advancement and Trends in Technology.	
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

BOOKS RECOMMENDED

1. Arvind Narayanan, Joseph Bonneau, Edward Felten, andrew Miller, Steven Goldfeder, “Bitcoin and Cryptocurrency Technologies: A Comprehensive introduction”, Princeton University Press, 2016.
2. Roger Wattenhofer, “Blockchain Science: Distributed Ledger Technology”, independently Published, ISBN-10 : 1793471738, 2019.

3. Andreas M. Antonopoulos, “Mastering Bitcoin: Programming the Open Blockchain”, Shroff/O'Reilly, 2017.
4. Elaine Shi, “Foundations of Distributed Consensus and Blockchains”, (URL: http://elaineshi.com/docs/blockchain-book.pdf), 2020.
5. Alan T. Norman, “Blockchain Technology Explained: the Ultimate Beginner s Guide About Blockchain Wallet, Mining, Bitcoin, Ethereum, Litecoin, Zcash, Monero, Ripple, Dash, IOTA and Smart Contracts”, Amazon Digital Services, 2017.

ADDITIONAL BOOKS RECOMMENDED

1. Bahga, Arshdeep, and Vijay Madisetti. "Blockchain applications: a hands-on approach", VPT, 2017.

Course Outcomes **At the end of the course, students will**	
CO1	have knowledge about the design principles of blockchain and smart contracts.
CO2	be able to program and demonstrate the working of different consensus mechanisms.
CO3	be able to deploy and interact with blockchain systems by setting up a system and sending and reading the transactions.
CO4	be able to design, build, and deploy distributed applications and smart contracts by identifying the need of blockchains to find the solution to the real-world problems.
CO5	be able to evaluate security, privacy, and efficiency of a given blockchain use case.
CO6	have knowledge about the challenges related to blockchain and smart contracts.

M. Tech. – I (CSE) ISP Semester – II	L	T	P	C
CSIS112: MACHINE LEARNING FOR SECURITY (CORE ELECTIVE-3 OR 4)	3	0	2	4

Course Objective	
1	to describe the fundamental concepts of machine learning for devising security mechanisms.
2	to enumerate the techniques for intrusion detection and malware detection and analysis using machine learning.
3	to learn the machine learning techniques for network traffic analysis
4	to analyse the machine learning approaches for security for probable abuse by the adversary.
5	to design secure machine learning based schemes for malware detection and intrusion detection.

INTRODUCTION & REVIEW OF THE MACHINE LEARNING BASICS	**(04 Hours)**
Review of the basic concepts in Linear Algebra, Probability and Statistics. Introduction to the ML techniques. Machine Learning problems viz. Classification, Regression, Clustering, Association rule learning, Structured output, Ranking. The Supervised and Unsupervised learning algorithms. Linear Regression, Gradient descent for convex functions, Logistics Regression and Bayesian Classification Support Vector Machines, Decision Tree and Random Forest, Neural Networks, DNNs , Ensemble learning. Principal Components Analysis. Un-supervised learning algorithms: K-means for clustering problems, K-NN (k nearest neighbors). Apriori algorithm for association rule learning problems. Generative vs Discriminative learning. Empirical Risk Minimization, loss functions, VC dimension. Data partitioning (Train/test/Validation), cross-validation, Biases and Variances, Regularization.	
MACHINE LEARNING FOR SECURITY	**(05 Hours)**
Introduction to Information Assurance. Review of Cybersecurity Solutions: Proactive Security Solutions, Reactive Security Solutions: Misuse/Signature Detection, Anomaly Detection, Hybrid Detection, Scan Detection. Profiling Modules. Understanding the Fundamental Problems of Machine-Learning Methods in Cybersecurity. Incremental Learning in Cyberinfrastructures. Feature Selection/Extraction for Data with Evolving Characteristics. Privacy-Preserving Data Mining. Motivation for ML in security with real-world case studies. Topics of interest in applications of machine learning for security.	
MACHINE LEARNING TECHNIQUES FOR INTRUSION DETECTION	**(08 Hours)**
Emerging Challenges in Cyber Security for Intrusion Detection: Unifying the Current Anomaly Detection Systems, Network Traffic Anomaly Detection. Imbalanced Learning Problem and Advanced Evaluation Metrics for IDS. Reliable Evaluation Data Sets or Data Generation Tools. Privacy Issues in Network Anomaly Detection. Machine Learning Techniques: for Anomaly Detection, for Misuse/Signature detection, for Hybrid detection, for Scan detection.Cost-Sensitive Modeling for Intrusion Detection. Data Cleaning and Enriched Representations for Anomaly Detection in System Calls.	
MACHINE LEARNING TECHNQIUES FOR MALWARE ANALYSIS	**(08 Hours)**
Emerging Cyber Threats in malwares: Threats from Malware, Botnets, Cyber Warfare, Mobile Communication. Cyber Crimes. Malware Analysis: Feature generation, Features to Classification. Taxonomy of malware analysis approaches based on machine learning. Malware Detection, Similarity Analysis, Category Detection. Feature Extraction. PE Features. Supervised, Unsupervised and Semi-supervised learning algorithms for Malware Detection. Using Deep Learning Approaches: Generative Adversarial Networks.	
NETWORK TRAFFIC ANALYSIS & WEB ABUSE DETECTION	**(08 Hours)**

Machine Learning for Profiling Network Traffic: Theory of Network defense (access control, authentication, detecting in-network attackers, data-centric security, honeypots), Predictive model for classifying network attacks.	
MACHINE LEARNING IN PRIVACY PRESERVATION	**(06 Hours)**
k-anonymity; l-diversity; deferentially private data storage/release; verifiable differential privacy; privacy-preserving inference of social networking data; privacy-preserving recommender system; privacy versus utility. Machine learning techniques for Privacy Preserving Data Mining.	
ADVERSARIAL MACHINE LEARNING	**(06 Hours)**
Adversarial Machine Learning: Motivation and Background. Practical Scenarios and Examples. Modelling the Adversary: Attack Surface Adversary Goals Adversary capabilities. Taxonomy of Adversarial Attacks on Machine Learning: Influence Specificity Security Violation. Data poisoning; Perturbation; Defense mechanism; Generative Adversarial Networks. A peep into Industry Perspectives: Theme of inference Secure Software Development Life Cycle or Secure Development Cycle. Key Inferences in terms of Security gaps, Suggested panacea.	
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**
	(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)

BOOKS RECOMMENDED

1. Clarence Chio, David Freeman., "Machine Learning and Security. Protecting Systems with Data and Algorithms", O'Reilly Media Publications, 2018.
2. Marcus A. Maloof (Ed.) , "Machine Learning and Data Mining for Computer Security: Methods and Applications", Springer-Verlag London Limited, 2006.
3. Sumeet Dua and Xian Du, "Data Mining and Machine Learning in Cybersecurity". CRC Press, Taylor and Francis Group, LLC. 2011.
4. Research Papers Prescribed in the class.
5. Fei Hu, Xiali Hei, "AI, Machine Learning and Deep Learning: A Security Perspective", United States: CRC Press, 2023.

Course Outcomes **At the end of the course, students will**	
CO1	have a knowledge of the limitations of the conventional security software in the wake of machine learning based attacks on the security software
CO2	be able to apply the concepts machine learning based intrusion detection to analyze the IDSs.
CO3	be able to analyze the malware analysis and mitigation based solutions for the probable threats therein.
CO4	be able to design the threat models based on machine learning approaches for network analysis.
CO5	be able to use the concepts of machine learning to prevent security design faults.

M. Tech. – I (CSE) ISP Semester – II	L	T	P	C
CSIS118: SOFTWARE SECURITY (CORE ELECTIVE-3 OR 4)	**3**	**0**	**2**	**4**

Course Objective	
1	to discuss and explain the fundamental concepts of software security and defensive programming.
2	to enumerate the vulnerabilities in a typical memory unsafe language and the potential attacks/exploits.
3	to learn counter mechanisms for preventing the security vulnerabilities from being exploited and those for ensuring secure programs.
4	to analyse the limits of the applicability of the sast tools as well as the dast tools.
5	to design a program free from the known vulnerabilities as well as to withstand the zero-day vulnerabilities.
6	to apply the skills learnt to generate secure programs.

INTRODUCTION	**(02 hours)**
Introduction to the course. Review of Information Security concepts. The CIA Triad. Systems Security, Information Security, Application Security, Network Security – commonalities and differences. Essential Terminologies. Proactive software security vis-à-vis the security software. The concept of Software Security. Security in Software Development Life Cycle. Security as a Software Quality attribute. The trinity of troubles viz. Connectivity, Extensibility and Complexity. Studies of various catastrophes due to Insecure software. Model Based Security Engineering, Three Pillars of Software Security. Security in Software Lifecycle. The basic terminologies: a bug, an exploit, a threat, defects, vulnerabilities, risks, attacks.	
SECURITY ATTACKS AND TAXONOMY OF SECURITY ATTACKS	**(02 Hours)**
Review of security attacks – Taxonomy of Security Attacks, Methods. Attacks in each phase of software life cycle. Attacks on the TCP/IP protocol suite layers. Motivation for attackers, Methods for attacks: Malicious code, Hidden software mechanisms, Social Engineering attacks, Physical attacks. Non-malicious dangers to software. Attacks in each phase of software life cycle. Security Vulnerabilities and Attack Taxonomy in Internet of Things and Cyber Physical Systems. Review of Malwares: Viruses, Trojans, and Worms. Malware Terminology: Rootkits, Trapdoors, Botnets, Key loggers, Honeypots. IP Spoofing, Tear drop, DoS, DDoS attacks.	
THE SECURITY VULNERABILITIES - I	**(10 Hours)**
The Software Vulnerabilities: Vulnerabilities in the Memory-safe and memory-unsafe languages. Introduction to the Program Stack Analysis. Hands-on on Stack Analysis using gcc compiler and gdb debugger tool. Methods of security attack exploiting the vulnerabilities in the code. Taxonomy of security vulnerabilities. Remote Code Execution. State-of-the-art in research in Security Vulnerabilities. Overview of C, C++, Java Security Vulnerabilities. The common Web vulnerabilities: the Buffer Overflow - Stack overflows, Heap Overflows, the Code and Command Injections and the types: SQL injection, Cross-site scripting, Interpreter injection; the Format String vulnerabilities, writing shellcode. The Seven Pernicious Kingdoms. The Hidden form fields, Weak session cookies. Fault injection & Fault monitoring, Fail open authentication The OWASP Top 25 vulnerabilities in the current year.	
CODE REVIEWS AND STATIC ANALYSIS OF THE SOURCE CODE	**(08 Hours)**
Introduction to Code reviews and Static Informal reviews, Formal inspections. Illustrations. Introduction to Code reviews and Static Analysis. Code Reviews. Static Code Analysis. Static and Dynamic Application	

Security Testing (SAST and DAST) tools. Using basic linting to detect security vulnerabilities in the code with the linux find(), grep(), awk(), splint() and the FlawFinder. A glance at Code Analyzer Tools : Top-10: Raxis, SonarQube for Code Quality and Code Security, PVS-Studio, reshift, Embold, SmartBear Collaborator, CodeScene Behavioral Code Analysis, RIPS Technologies. Others: Cscope, Ctags, Editors, Cbrowser	
THE SECURITY VULNERABILITIES – II	**(09 Hours)**
Introduction to Session Management in Web Applications. Session Management best practices. The XSRF (Cross-site Request Forgery) Attack. Security vulnerabilities in Java: Connection String Injection, LDAP Injection, Reflected XSS, Resource Injection, Persistent XSS attacks in Java, The XPath Injection. Insecure deserialization, Remote code execution (RCE). Log injection. Mail injection. Vulnerabilities in Java libraries. Vulnerabilities in the Java sandboxing mechanism. Insufficient Transport Layer Protection (ITLP). Application misconfiguration and Software Composition Analysis (SCA).	
THREAT MODELLING	**(10 Hours)**
Finding Threats: Using STRIDE, Attack Patterns, Attack Trees, Misuse Patterns. Threat modelling with Attack Trees and Graphs. Anti-models. State transition diagrams. Access control models. Specifying Secrecy, Authentication and Assertions. Graph based specifications, UML-based specifications. Formal Security specifications. Web Threats, Cloud Threats, Mobile Threats, Threats to Cyrptosystems. Attack Libraries: Properties, OWASP Top Ten, CAPEC. Privacy Tools: Solove's Taxonomy of Privacy, Privacy Considerations for Internet Protocols, Privacy Impact Assessments (PIA), The Nymity Slider and the Privacy Ratchet, Contextual Integrity, LINDDUN. Threat Modeling tools: Whitebiards, Office-suites, Bug-tracking systems, TRIKE, Sea-monster, Elevation-of-privilege, Threat Modeler, Microsoft's SDL Threat Modeling Tool. When to Threat Model, What to model, Scenario-Specific Elements of Threat Modeling. Automated Threat Modeling, Threat modeling with code.	
DYNAMIC APPLICATION SECURITY TESTING	**(04 Hours)**
Basics, Approaches to DAST, DAST application analysis. DAST prerequisites. DAST job order, DAST run options. Tools, DAST Pros and Cons. DAST in DevOps practices. Interactive application security testing (IAST), Software composition analysis (SCA).	
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**
	(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)

BOOKS RECOMMENDED

1. Michael Howard, David LeBlanc, “Writing Secure Code”, Microsoft Press, 2nd Edition. 2004.
2. McConnell Steve, “Code Complete (Developer Best Practices)”, Kindle Edition, Microsoft Press, 2nd Edition. 2004.
3. Edward Skoudis, Tom Liston, “Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defences”, Prentice Hall.
4. Mark G. Graff, Kenneth R.VanWyk, “Secure Coding: Principles and Practices”, O'Reilly Media.
5. Gary McGraw, “Software Security: Building Security In”, Addison-Wesley.

ADDITIONAL BOOKS RECOMMENDED

1. Stuart McClure, Joel Scambray, George Kurtz , “Hacking Exposed 7: Network Security Secrets & Solutions”, McGraw-Hill Osborne Media.

Course Outcomes **At the end of the course, students will**	
CO1	have a knowledge of the basic concepts and problems of memory unsafe and memory safe languages
CO2	be able to use the concepts to detect security vulnerabilities and prevent them.
CO3	be able to analyze/interpret program code for doing Static and Dynamic Security Testing.
CO4	be able to design the new software with the security features builtin rather than reliance on the security software.
CO5	be able to use the concepts of information security to prevent security design faults.

M. Tech. – I (CSE) ISP Semester – II	L	T	P	C
CSIS120: SECURITY AND PRIVACY IN THE RESOURCE CONSTRAINED ENVIRONMENTS (CORE ELECTIVE-3 OR 4)	3	0	2	4

Course Objective	
1	to be able to understand the concept of resource constrained devices, their characteristics, their applications and the constraints under which they operate.
2	to be able to understand the importance of the security issues in embedded devices/systems, with wireless sensor networks (wsns) and the internet of things (iot) as the case studies.
3	to be able to understand the wireless sensor networks, the typical configurations of the constituent components viz. sensor motes, typical applications, operating environments, programming languages, simulators through demonstrations.
4	to be able to analyze the security vulnerabilities with respect to various denial of service attacks at the network layer in wsns as well as that in the routing protocols for the manets.
5	to be able to analyze the design of a typical link layer security architecture for wsns and the design of the light weight ciphers for the wsns.
6.	to be able to design the security mechanisms suitable for wsns viz. the iv, mac, replay protection algorithm, key deployment algorithm for the hop-by-hop as well as end-to-end secure data aggregation protocols.
7.	to be able to analyze the advanced key management techniques viz. attribute based encryption, identity based encryption, function encryption and their applications.

INTRODUCTION	**(03 Hours)**
Review of the Network Security Concerns. Fundamental Network Security Threats. Types of Network Security Threats. Network Security Vulnerabilities, their types: Technological Vulnerabilities, Configuration Vulnerabilities, Security policy Vulnerabilities. Types of Network Security Attacks.	
UBIQUITOUS AND PERVASIVE COMPUTING PARADIGM EMBEDDED SECURITY	**(06 Hours)**
Introduction to ubiquitous and pervasive computing paradigm, Embedded systems, Wireless Sensor Nodes as representative Embedded Systems, Wireless Sensor Networks (WSNs), Typical configurations, Typical Applications of the WSNs. Case studies of real world applications. Deployment models, Characteristics, Security Issues in Wireless Sensor Networks, Typical Attacks and Countermeasures.	
SECURE DATA AGGREGATION	**(12 Hours)**
The Concept of In Network processing and Data Aggregation. Motivation for the Link Layer Security architecture in Wireless Sensor Networks. Design Issues for Link Layer Security in Wireless Sensor Networks. Case studies of the hop-by-hop security architectures viz. TinySec, MiniSec, FlexiSec. Use of TOSSIM, Avrora or any other appropriate simulator. End-to-end security architecture for Wireless Sensor Networks.	
END-TO-END SECURE DATA AGGREGATION & ALGORITHMS	**(12 Hours)**
Use of Partial Homomorphic Encryption Algorithms – Case studies. Additive and Multiplicative Homomorphic Encryption algorithms. Robustness and Resilient Concealed Data Aggregation: Different approaches to offer data integrity viz. using conventional MAC - Aggregate MAC, Homomorphic MAC, Hybrid Secure Data Aggregation. Malleability Resilient Concealed Data Aggregation	
SECURITY OF THE ROUTING PROTOCOLS IN MANETS	**(02 Hours)**
Routing Protocols for MANETS, Their Security Vulnerabilities, Typical Solutions. Security of the AODV protocol – typical mitigation to counter Black-hole attacks ON AODV.	

THE KEY MANAGEMENT IN THE EMBEDDED SYSTEMS	**(04 Hours)**
Public Key Infrastructure in Wireless Sensor Networks, The TinyPK protocol as a case study. Public Key Infrastructure in Wireless Sensor Networks, The Merkle-Hellman tree based approach for key validation. Attribute Based Encryption and its motivation for Embedded Systems. Identity-based encryption and Functional encryption, motivation and case studies.	
THE TINY CIPHERS	**(02 Hours)**
Design of the STATE OF THE ART tiny ciphers for the tiny devices and the RFID devices: TEA, XTEA, XXTEA, KTANTAN, mCrypton etc.	
THE INTERNET OF THINGS SECURITY	**(04 Hours)**
The Internet of Things. Architecture. Constituent Elements. The Security and Privacy Issues in IoT Systems. Overview of the IoT Protocols. Security of the RPL protocol. The IoT Security Protocols viz. ZigBee, Bluetooth, 6LowPAN, RPL. The CoAP.	
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

BOOKS RECOMMENDED
1. The research papers prescribed in the class.

Course Outcomes: **At the end of the course, students will be able**	
CO1	to understand the concept of resource constrained devices, their characteristics, their applications and the constraints under which they operate.
CO2	to apply the security mechanism for resource constraints environments and identify the security vulnerabilities with respect to various Denial of Service attacks at the Network Layer in WSNs as well as that in the Routing protocols for the MANETs.
CO3	to analyze the design of a typical link layer security architecture for WSNs and the design of the light weight ciphers for the WSNs.
CO4	to evaluate the advanced key management techniques viz. Attribute Based Encryption, Identity Based Encryption, Function Encryption and their applications
CO5	to design the security mechanisms suitable for WSNs viz. the IV, MAC, replay protection algorithm, key deployment algorithm for the hop-by-hop as well as end-to-end Secure Data Aggregation protocols.

M. Tech. – I (CSE) ISP Semester – II	L	T	P	C
CSIS122: SECURITY AND PRIVACY IN SOCIAL NETWORKS (CORE ELECTIVE-3 OR 4)	3	0	2	4

Course Objective	
1	to understand online social media privacy and security issues.
2	to recognize different privacy and security problems on online social media (spam, phishing, fraud nodes, and identity theft).
3	to use online social networks to express a wide range of problems.
4	to use the analysis of security issues and countermeasures to create new knowledge, decisions, and actions.
5	to solve identity problems with understanding of location based privacy.

INTRODUCTION TO SOCIAL NETWORKS SECURITY	**(06 Hours)**
Types and Classification of Social Media, Problems and Opportunities of Social Media- Risks of Social Media, Public Embarrassment, False Information, Information Leakage, Retention and Archiving Content, Backing Up Social Media, Loss of Data/Equipment, Dark Side of Social Media, Cybercrime, Social Engineering, Hacked Accounts; Sharing Information on Social Media.	
ATTACKS ON SOCIAL MEDIA AND DATA ANALYTICS SOLUTIONS	**(06 Hours)**
Malware and Attacks, Types of Malware, Threats to Cyber Security, Attacks on Social Media, Data Analytics Solutions, Data Mining for Cyber Security, Malware Detection as a Data Stream Classification Problem, Cloud-Based Malware Detection for Evolving Data Streams, Cloud Computing for Malware Detection, Design and Implementation of the System Ensemble Construction and Updating, Malicious Code Detection.	
CONFIDENTIALITY, ACCESS CONTROL, PRIVACY AND TRUST IN SOCIAL MEDIA	**(08 Hours)**
CPT Framework and Process, Inference Engines, Confidentiality Management, Privacy for Social Networks, Trust for Social Networks, Security Policies for Social Networks, Access Control System for Social Networks	
INFERENCE CONTROL FOR SOCIAL MEDIA	**(06 Hours)**
Architecture and Design of an Inference Controller, Inference Control through Query Modification - Query Modification, Query Modification With Relational Data, Sparql Query Modification, Query Modification for Enforcing Constraints, Applications, Use Cases of Inference Controller.	
SECURE QUERY PROCESSING FOR SOCIAL MEDIA	**(06 Hours)**
Secure Cloud Query Processing with Relational Data for Social Media, Secure Cloud Query Processing for Semantic Web-Based Social Media - Access Control and System Architecture.	
SOCIAL NETWORK INTEGRATION AND ANALYSIS WITH PRIVACY PRESERVATION	**(09 Hours)**
Social Network Analysis, Limitations of Current Approaches for Privacy-Preserving Social Networks - Privacy Preservation of Relational Data, K-Anonymity and L-Diversity, Privacy Preservation of Social Network Data, Framework of Information Sharing and Privacy Preservation For Integrating Social Networks - Sharing Insensitive Information, Generalization, Probabilistic Model of Generalized Information, Integrating Generalized Social Network For Social Network Analysis Task.	
Advanced Topics	**(04 Hours)**
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

BOOKS RECOMMENDED

1. Thuraisingham B., Abrol Raymond Heatherly S., Kantarcioglu M., Khadilkar V., Khan L, "Analyzing and Securing Social Networks", Taylor & Francis Group, 2016.
2. Michael Cross, "Social Media Security", Elsevier, 2013
3. Altshuler Y., Elovici Y., Cremers A.B., AharonyN., Pentland, "Security and Privacy in Social Networks", Springer, 2013.
4. Gavin Bell, "Building Social Web Applications",O'Reilly, 2009.
5. Carminati, B., Ferrari, E., Viviani, M, " Security and Trust in Online Social Networks" , Switzerland: Morgan & Claypool Publishers, 2013.

Course Outcomes **At the end of the course, students will**	
CO1	be able to understand various privacy and security risks (spam, phishing, fraud nodes, identity theft).
CO2	be able to apply the appropriate analytical methodology for fresh research and evaluate the results accurately.
CO3	be able to analyse fraudulent entities in online social networks.
CO4	be able to evaluate algorithms for handling various concerns comprehensively on online Social Media.
CO5	be able to design the system addressing various privacy issues of frameworks to relate them to techniques and applications.

M. Tech. – I (CSE) ISP Semester – II	L	T	P	C
CSIS126: ADVERSARIAL MACHINE LEARNING (CORE ELECTIVE-3 OR 4)	**3**	**0**	**2**	**4**

Course Objective	
1	to be able to understand the concept of trustworthy machine learning.
2	to be able to understand various types of attacks and defences in adversarial machine learning.
3	to be able to understand the issues faced by the applications using machine learning.
4	to be able to analyze the relationship between the information leakage and privacy.
5	to be able to analyze and do research while learning about adversarial machine learning.

INTRODUCTION	**(03 Hours)**
Introduction, Background, review of the concepts of machine learning for security. Motivation for studying Adversarial Machine Learning through various case studies.	
ADVERSARIAL LEARNING	**(05 Hours)**
Adversarial Classification, Adversarial Learning, Generative Adversarial Networks.	
PRIVACY ATTACKS (ADVERSARIAL EXAMPLES) & COUNTER MECHANISMS	**(10 Hours)**
Stealing Machine Learning Models via Prediction APIs, Model Reconstruction from Model Explanations, Membership Inference Attacks Against Machine Learning Models. Counter Mechanisms: Machine Learning with Membership Privacy using Adversarial Regularization. Privacy-preserving Prediction. Deep Learning with Differential Privacy	
POISONING ATTACKS (ADVERSARIAL EXAMPLES) & COUNTER MECHANISMS	**(10 Hours)**
Poisoning Attacks, Poisoning Attacks against Support Vector Machines, Poison Frogs, Targeted Clean-Label Poisoning Attacks on Neural Networks, Stronger Data Poisoning Attacks Break Data Sanitization Defenses, Transferable Clean-Label Poisoning Attacks on Deep Neural Nets. Counter mechanisms.Certified Defenses for Data Poisoning Attacks. Robust Training of Deep Neural Networks with Extremely Noisy Labels. Robust Logistic Regression and Classification.	
EVASION ATTACKS (ADVERSARIAL EXAMPLES) & COUNTER MECHANISMS	**(10 Hours)**
Explaining and Harnessing Adversarial Examples. Towards Evaluating the Robustness of Neural Networks Why Do Adversarial Attacks Transfer? Explaining Transferability of Evasion and Poisoning Attacks.	
ADVANCED ADVERSARIAL ATTACKS & COUNTER MECHANISMS	**(07 Hours)**
Understanding Black-box Predictions via Influence Functions. Machine Learning with Adversaries: Byzantine Tolerant Gradient Descent. Comprehensive Privacy Analysis of Deep Learning: Passive and Active White-box. Inference Attacks against Centralized and Federated Learning. Towards Deep Learning Models Resistant to Adversarial Attacks. Certified Defenses against Adversarial Examples. An abstract domain for certifying neural networks. Adversarially Robust Generalization. Adversarial Examples Not as Bugs. Theoretically Principled Trade-off between Robustness and Accuracy. Industry Perspectives.	
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

BOOKS RECOMMENDED
1. The research papers prescribed in the class.

Course Outcomes **At the end of the course, students will be able**	
CO1	to understand the taxonomy of the adversarial attacks.
CO2	to apply the adversarial use cases of machine learning applications.
CO3	to analyze the limitations of the conventional machine learning techniques in defending against the adversarial attacks.
CO4	to evaluate different security mechanism for adversarial machine learning.
CO5	to design the security mechanisms in a machine learning application to withstand the adversarial attacks.

M. Tech. – I (CSE) ISP Semester – II	L	T	P	C
CSIS128: MOBILE SECURITY AND PENETRATION TESTING (CORE ELECTIVE-3 OR 4)	**3**	**0**	**2**	**4**

Course Objective	
1	to understand the importance of security issues in mobile applications.
2	to enumerate the security vulnerabilities and exploits in the given applications on the android and the ios platforms.
3	to learn how the vulnerabilities are used to create an exploit for the applications on the android and the ios platforms.
4	to analyse software applications on the android and the ios platforms for the security issues therein.
5	to design the secure code and applications for the android and the ios platforms.
6	to apply the knowledge acquired to implement secure software for the android and the ios platforms.

BACKGROUND & INTRODUCTION	**(03 Hours)**
Introduction to the course. Review of the Mobile Application Security Landscape. The SmartPhone Market. The Android and iOS Operating Systems. Public Android and iOS Operating Systems Vulnerabilities. Key Challenges. Mobile Application Penetration Testing Methodology. The OWASP Mobile Security Project.	
THE ANDROID AND THE IOS ARCHITECTURES & TEST ENVIRONMENTS.	**(07 Hours)**
The Linux Kernel, the Android and the IOS architectures, the Java Virtual Machine, Core Java Libraries, The Application Layer and the application framework. The Android Application Components. The IOS Application Programming Languages, IOS Security Model. Hardware Level Security and Jailbreaking. The Mach-O binary file format. Mobile app penetration testing environment setup. The Android Studio and SDK. Genymotion. Configuring the emulator for http proxy. Google Nexus-5 physical device. SSH clients. Various tools in the IoS: Cydia, BigBoss, Darwins, iPA Installer, tcpdump, ios SSL Kill-switch. Emulators and simulators.	
MOBILE PENETRATION TOOLS	**(08 Hours)**
Android Security Tools: APKAnalyzer, The drozer tool, APKTool, the dex2jar API, JD-GUI, Androguard, Working with the Java debugger. iOS Security Tools: oTool, SSL Kill-switch, The Keychain dumper, LLDB, Clutch, Class-dump-z, Cycript, Frida, Hopper, Snoop-it.	
THREAT MODELLING A MOBILE APPLICATION	**(10 Hours)**
Basic concepts of threat modelling, Threats, Vulnerabilities, Risks. Approaches to Threat Model. Threat Agents in the mobile applications. How to create a threat model ? Using STRIDE, PASTA, Trike in Mobile Applications. Building Attack Plans, Threat Trees, Using Attack Patterns for Mobile Applications. Risk Assessment Models.	
ATTACKING ANDROID AND IOS APPLICATIONS	**(09 Hours)**
Attacking Android Applications: Setting up the target app. Analyzing apps using tools. Attacking activities, services, broadcast receivers, content providers, WebViews, SQL Injection, Man-in-the-middle attacks, SSL Spinning, Hardcoded credentials. Storage/archive analysis. Log analysis. Binary Patching. Attacking iOS applications: Setting up the target app. Storage/archive analysis. Reverse Engineering. Static code analysis. App patching, Runtime manipulation using. Cycript. Dumpdecrypted. Client-side injections. Man-in-the-middle attacks, SSL cert pinning. Building a remote tracer using LLDB	

SECURING ANDROID AND IOS APPLICATIONS.	**(08 Hours)**
Secure by design. Secure mind map for developers. Device level, platform level, application level protection. iOS cookie and keychains, App Storage protection. Application permissions.Securing Webview. Binary protection. Network level protection. OWASP mobile app security checklist. Secure coding Best practices for Android, iOS.	
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

BOOKS RECOMMENDED

1. Vijay Kumar Velu, “Mobile Application Penetration Testing” , Packt Publishing Limited, 2016.
2. Jeff McWherter, Scott Gowell, “Professional Mobile Application Development”, Wrox Publications, 2012.
3. David Thiel ,“iOS Application Security: The Definitive Guide for Hackers and Developers”, No Starch Press, 2016.
4. David Rogers , “Mobile Security: A Guide for Users”, Lulu.com publishers 2013.
5. Kunal Relan , “ iOS Penetration Testing: A Definitive Guide to iOS Security”, Apres Publications, 2017.

Course Outcomes **At the end of the course, students will**	
CO1	The student will be able to identify the security issues in Android and iOS applications, using a wide variety of techniques including Reverse Engineering, Static/Dynamic/Runtime and Network Analysis.
CO2	The student will be able to code simple iOS and Android applications.
CO3	The student will be able to identify the vulnerabilities in the existing software, be able to decrypt and disassemble application
CO4	The student will be able to fully work exploits and malicious applications and thereby be able to learn the mitigation of the exploits.
CO5	The student will be able to design secure mobile applications.

M. Tech. – I (CSE) ISP Semester – II	L	T	P	C
CSIS130: SECURE SOFTWARE ENGINEERING (CORE ELECTIVE-3 OR 4)	**3**	**0**	**2**	**4**

Course Objective	
1	to understand the limitations of the security software and the motivation of designing secure software based on engineering principles.
2	to enumerate the security attacks at the various layers of the tcp/ip protocol suite as well as in the different phases of the sdlc.
3	to learn the common weaknesses in the memory unsafe and memory safe languages.
4	to analyse the code using static and dynamic analysis tools for security testing.
5	to design a secure model of the software using the attack trees, attack patterns and extensions to the uml for security.
6	to apply the principles learnt throughout the requirements analysis, specifications, design and implementation of the software.

INTRODUCTION	**(02 Hours)**
Introduction to the course. Review of Information Security concepts. The CIA Triad. Systems Security, Information Security, Application Security, Network Security – commonalities and differences. Essential Terminologies. Secure Software & its properties. Security Software: Critical shortcomings. Studies of various catastrophes due to Insecure software. What is Software Security? Software Assurance? Motivation for Software Security. Software Security vs Security Software. The trinity of troubles viz. Connectivity, Extensibility and Complexity. Model Based Security Engineering. Security in Software Development Lifecycle (SDLC). Software Security Best Practices applied to various software artifacts in the SDLC. Addressing security throughout the SDLC. Three Pillars of Software Security. Software Security Touchpoints.	
SECURITY ATTACKS AND TAXONOMY OF SECURITY ATTACKS	**(02 Hours)**
Review of security attacks – Taxonomy of Security Attacks, Methods. Attacks in each phase of the software life cycle. Attacks on the TCP/IP protocol suite layers. Motivation for attackers, Methods for attacks: Malicious code, Hidden software mechanisms, Social Engineering attacks, Physical attacks. Non-malicious dangers to software. The Denial of Service Attacks in each phase of the software life cycle. Security Vulnerabilities and Attack Taxonomy in Internet of Things and Cyber Physical Systems. Review of Malwares: Viruses, Trojans, and Worms. Malware Terminology: Rootkits, Trapdoors, Botnets, Keyloggers, Honeypots. IP Spoofing, Tear drop, DoS, DDoS attacks.	
THE SOFTWARE VULNERABILITIES	**(09 Hours)**
The Software Vulnerabilities: Vulnerabilities in the Memory-safe and memory-unsafe languages. Introduction to the Program Stack Analysis. Hands-on on Stack Analysis using gcc compiler and gdb debugger tool. Methods of security attack exploiting the vulnerabilities in the code. Taxonomy of security vulnerabilities. Remote Code Execution. State-of-the-art in research in Security Vulnerabilities. Overview of C, C++, Java Security Vulnerabilities.	
THE WEB VULNERABILITIES & COUNTERMEASURES	**(09 Hours)**
The common Web vulnerabilities: the Buffer Overflow - Stack overflows, Heap Overflows, the Code and Command Injections and the types: SQL injection, Cross-site scripting, Interpreter injection; the Format String vulnerabilities, writing shellcode. The Seven Pernicious Kingdoms. The Hidden form fields, Weak session cookies. Fault injection & Fault monitoring, Fail open authentication The OWASP Top 25 vulnerabilities in the current year.	
THE WEB VULNERABILITIES IN MEMORY SAFE LANGUAGES & COUNTERMEASURES	**(09 Hours)**

Introduction to Session Management in Web Applications. Session Management best practices. The XSRF (Cross-site Request Forgery) Attack. Security vulnerabilities in Java: Connection String Injection, LDAP Injection, Reflected XSS, Resource Injection, Persistent XSS attacks in Java, The XPath Injection. Insecure deserialization, Remote code execution (RCE). Log injection. Mail injection. Vulnerabilities in Java libraries. Vulnerabilities in the Java sandboxing mechanism. Insufficient Transport Layer Protection (ITLP). Application misconfiguration and Software Composition Analysis (SCA).
CODE REVIEWS AND STATIC ANALYSIS OF THE SOURCE CODE **(04 Hours)**
Introduction to Code reviews and Static Informal reviews, Formal inspections. Illustrations. Introduction to Code reviews and Static Analysis. Code Reviews. Static Code Analysis. Static and Dynamic Application Security Testing (SAST and DAST) tools. Using basic linting to detect security vulnerabilities in the code with the linux find(), grep(), awk(), splint() and the FlawFinder. A glance at Code Analyzer Tools : Top-10: Raxis, SonarQube for Code Quality and Code Security, PVS-Studio, reshift, Embold, SmartBear Collaborator, CodeScene Behavioral Code Analysis, RIPS Technologies. Others: Cscope, Ctags, Editors, Cbrowser. Comparison with the Dynamic Application Security Testing.
THREAT MODELLING **(06 Hours)**
Finding Threats: Using STRIDE, Attack Patterns, Attack Trees, Misuse Patterns. Threat modelling with Attack Trees and Graphs. Anti-models. State transition diagrams. Access control models. Specifying Secrecy, Authentication and Assertions. Graph based specifications, UML-based specifications. Formal Security specifications. Web Threats, Cloud Threats, Mobile Threats, Threats to Cyrptosystems. Attack Libraries: Properties, OWASP Top Ten, CAPEC. Threat Modeling tools: Secure Design – Principles: Secure Software Design Principles and Practices. Security Architectures. Design oriented, Goal oriented and Problem oriented approaches. Security Patterns: Modelling and Classification of Security Patterns. Patterns characterization. Security Design Approaches viz. UML, Secure UML, UMLSec and Misuse cases. Illustrating the design of a security protocol.
SECURITY IN DESIGN **(04 Hours)**
Secure Design – Principles: Secure Software Design Principles and Practices. Security Architectures. Design oriented, Goal oriented and Problem oriented approaches. Security Patterns: Modelling and Classification of Security Patterns. Patterns characterization. Security Design Approaches viz. UML, Secure UML, UMLSec and Misuse cases. Illustrating the design of a security protocol.
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.) **(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)

BOOKS RECOMMENDED

1. Andrew Magnusson, “Practical Vulnerability Management: A Strategic Approach to Managing Cyber Risks, No Starch Press,2020.
2. H Mouratidis, “ Software Engineering for Secure Systems – Industrial and Research Perspectives. Information Science Reference”, IGI global, 2011.
3. Gary McGraw, “Software Security : Building Security In”,Addison Wesley Software Security Series, 2006 edition.
4. Theodor Richardson, Charles Thies, “Secure Software Design”, Jones and Bartlet Learning, 2013
5. McDonald, Malcolm, “Web Security for Developers: Real Threats, Practical Defense”, United States, No Starch Press, 2020.

ADDITIONAL BOOKS RECOMMENDED

1. Palmer, Steven, “Web Application Vulnerabilities: Detect, Exploit, Prevent”, United States, Elsevier Science, 2011.

2. Tarandach, Izar, and Coles, Matthew J, “Threat Modeling”, India, O'Reilly Media, 2020.
3. Janca, Tanya, “Alice and Bob Learn Application Security”, United Kingdom, Wiley, 2020.

Course Outcomes **At the end of the course, students will**	
CO1	have a knowledge of the limitations of the security software and the need for the software security
CO2	be able to apply the concepts of software security learnt, to detect security vulnerabilities and prevent them.
CO3	be able to analyze the security issues in the Requirements, in the Specifications, in the Design and that in the software code.
CO4	be able to design the threat models and security mis-use case diagrams to model the security threats the software being developed.
CO5	be able to use the concepts of information security to prevent security design faults.

M. Tech. – I (CSE) ISP Semester – II	L	T	P	C
CSIS132: FOUNDATIONS OF PRIVACY ENGINEERING (CORE ELECTIVE-3 OR 4)	**3**	**1**	**0**	**4**

Course Objective	
1	to understand the privacy violations and the underlying causes.
2	to learn limitations of statistical disclosure.
3	to integrate privacy into the software engineering lifecycle phases
4	to collect, analyze and reconcile system requirements in a privacy-sensitive ecosystem
5	to evaluate software designs based on privacy principles and privacy requirements.

INTRODUCTION	**(09 Hours)**
Course Overview and Conceptual Privacy Frameworks. Fair Information Principles. Privacy in Context. Informational Privacy. The Constitutional Right to Privacy. Reductionism vs. Coherentism. Critiques of Privacy. Meaning and Value of Privacy. The Scope of Privacy. Privacy and Technology. Privacy as Contextual Integrity. A Taxonomy of Privacy. Privacy Technologies: Secret sharing and DC nets. The Dining Cryptographers Problem. Mix networks and onion routing. Untraceable Electronic Mail. Tor: The Second-Generation Onion Router. Anonymous communication. Oblivious Transfer and Garbled Circuits. How to Exchange Secrets with Oblivious Transfer. Yao's Garbled Circuits. Evaluating encrypted neural networks	
DATA USE ON THE WEB	**(06 Hours)**
Privacy and Contextual Integrity: Framework and Applications. Summary of the HIPAA Privacy Rule (Permitted Uses and Disclosures, Authorized Uses and Disclosures). A Formalization of HIPAA for a Medical Messaging System. Experiences in the Logical Specification of the HIPAA and GLBA Privacy Laws	
PRIVACY IN REQUIREMENTS	**(10 Hours)**
Requirements: Expressing, Analyze system and privacy requirements using natural language use cases and semi-formal models. Conflicts reconciliation between system requirements and privacy requirements. Sources of requirements, trace matrices to manage compliance. Legal or regulatory requirements, privacy principles, privacy patterns and privacy controls. Goal-based analysis to refine privacy goals into functional, privacy-enhancing system specifications. Privacy threat and risk analysis to apply different risk models to explore privacy threats, vulnerabilities and mitigations, including: a legal compliance model, a FIPs-based model, Calo's subjective/objective harms model, Solove's privacy harms taxonomy, and Nissenbaum's Contextual Integrity.	
PRIVACY IN DESIGN	**(10 Hours)**
Privacy by design. Alternative design strategies to implement requirements. Architecture vs. Policy - Boundary between engineering automation and human reliance. Translation of policy into system specifications. Data Lifecycle: collection, use, and retention to transfer. Designing for various privacy qualities, including collection and use limitation, data minimization, anonymization or de-identification, destruction, and individual participation, among others. Evolution & Adaptability affecting privacy, including deployment, maintenance and upgrades that risk privacy requirements violation.	
TESTING FOR PRIVACY	**(10 Hours)**
Testing and Validation. TESTING privacy requirements. Accommodating requirements that are not easily tested, privacy-protective activities. Code reviews and code audits, and auditing runtime behavior.	

Tutorial Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(15 Hours)**
(Total Contact Time: 45 Hours + 15 Hours = 60 Hours)	

BOOKS RECOMMENDED

1. Axel van Lamsweerde, "Requirements Engineering: From System Goals to UML Models to Software Specifications" , John Wiley & Sons, Inc. 2009.
2. Vicenç Torra, "Data Privacy: Foundations, New Developments and the Big Data Challenge", Springer, 1st Edition, 2017.
3. The research papers prescribed in the class.
4. Stanford Encyclopedia of Philosophy: Article on Privacy, First Published, 2002. Substantive revision 2018.
5. Stallings, William, " Information Privacy Engineering and Privacy by Design: Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices", United Kingdom, Pearson Education, 2019.

Course Outcomes **At the end of the course, students will be able**	
CO1	To understand the privacy framework and principles
CO2	to integrate privacy into the software engineering lifecycle phases
CO3	to collect, analyze and reconcile system requirements in a privacy-sensitive ecosystem
CO4	to evaluate software designs based on privacy principles and privacy requirements
CO5	to interface with software developers on critical privacy issues

M. Tech. – I (CSE) ISP Semester – II	L	T	P	C
CSIS134: BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES (CORE ELECTIVE-3 OR 4)	3	0	2	4

Course Objective	
1	to demonstrate a familiarity with the fundamentals of cryptocurrencies.
2	to understand different cryptographic primitives and their use in the design of cryptocurrencies.
3	to analyse different cryptocurrencies and to assess the pros and cons of different cryptocurrencies.
4	to design decentralized applications that operates using cryptocurrencies.
5	to propose and evaluate different use cases of cryptocurrencies.

FUNDAMENTALS OF BLOCKCHAIN TECHNOLOGY AND CRYPTOGRAPHY	(09 Hours)
Centralization vs. Decentralization, Distributed Consensus, Consensus Without Identity, Blockchain, Incentives and Proof of Work, Digital Signature, Tamper Proof Ledger, Distributed Consensus, Proof of Work, Mining and Currency Supply, Cryptographic Hash Functions, Hash Pointers and Data Structures, Digital Signatures, Public Keys as Identities	
BITCOIN - A CRYPTOCURRENCY	**(10 Hours)**
Bitcoin Transactions, Bitcoin Scripts, Applications of Bitcoin Scripts, Bitcoin Blocks, Bitcoin Network, Peer-to-Peer Network Architecture, Limitations & Improvements, Bitcoin Mining, Consensus, Decentralized Consensus, Mining Nodes, Bitcoin Addresses, Wallets, Alternative Chains, Bitcoin Security, Ways to Store and Use Bitcoins	
ETHEREUM	**(10 Hours)**
Ethereum and Turing Completeness, Wallet, Transactions, Metamask, Ether, Externally Owned Accounts (EOAs) and Contracts, Block Explorer, Ethereum Clients, Ethereum Networks, Smart Contracts and Solidity, Smart Contract Security, Ethereum Virtual Machine, Comparison of Bitcoin and Ethereum.	
OTHER CRYPTOCURRENCIES	**(09 Hours)**
Stellar: Stellar Network, Consensus Protocol, Ledger Format, Transactions, Smart Contracts, Monero: Cryptonote protocol, Transactions, Mining, Ring Signatures, Zcash: Zero Knowledge Proofs, Mining, Comparison between Bitcoin, Ethereum, Monero, Zcash, and Other Cryptocurrencies.	
FINTECH AND APPLICATIONS	**(07 Hours)**
Hot and Cold Storage, Splitting and Sharing Keys, Online Wallets and Exchanges, Payment Services, Transaction Fees, Currency Exchange Markets, Building the Blockchain, Crypto Finance, Business Use Cases, Blockchain in Gaming, Investing in Blockchain, Government and Regulation, FinTech.	
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

BOOKS RECOMMENDED

1. Andreas M. Antonopoulos, “Mastering Bitcoin: Programming the Open Blockchain”, Shroff/O'Reilly, 2017.
2. Antonopoulos, Andreas M. and Wood, Gavin, “Mastering Ethereum”, O’Reilly Media, Inc., 2018.
3. Arvind Narayanan, Joseph Bonneau, Edward Felten, andrew Miller, Steven Goldfeder, “Bitcoin and Cryptocurrency Technologies: A Comprehensive introduction”, Princeton University Press,

2016.
4. Franco, Pedro, " Understanding Bitcoin: Cryptography, engineering and economics", John Wiley & Sons, 2014.
5. Elrom, Elad, "The blockchain developer: A Practical Guide for Designing, Implementing, Publishing, Testing, and Securing Distributed Blockchain-based Projects" , Apress, 2019.

ADDITIONAL BOOKS RECOMMENDED

1. Roger Wattenhofer, "Blockchain Science: Distributed Ledger Technology", independently Published, ISBN-10 : 1793471738, 2019.

Course Outcomes **At the end of the course, students will**	
CO1	have knowledge about the design principles of blockchain and cryptocurrencies.
CO2	be able to program and demonstrate the working of different consensus mechanisms.
CO3	be able to analyse Cryptocurrency transactions, scripts, and network.
CO4	be able to design decentralized applications that relies on cryptocurrencies.
CO5	be able to analyse the strengths and weaknesses of various cryptocurrencies.

M. Tech. – I (CSE) ISP Semester – II	L	T	P	C
CSIS136: ADVANCED CRYPTOGRAPHY (CORE ELECTIVE-3 OR 4)	3	0	2	4

Course Objective	
1	to demonstrate a familiarity with concepts related to number theory and apply them in modern cryptography.
2	to analyse the design of the state-of-the-art cryptosystems and assess their strengths and weaknesses.
3	to apply the knowledge of cryptography to solve real-world problems in the area of multi-party computation, secure storage at third party servers, etc.
4	to understand and analyze the design of advanced cryptosystems related to lattice-based cryptography, homomorphic encryption, and attribute-based encryption.

INTRODUCTION	**(05 Hours)**
One-way Functions (OWFs), Pseudorandom Generators (PRGs), Pseudorandom Functions (PRFs), Pseudorandom Permutations (PRSs), The Blum-Micali PRG and hybrid arguments, The Goldreich-Goldwasser-Micali PRF construction.	
SYMMETRIC CRYPTOGRAPHY	**(05 Hours)**
Symmetric Cryptography, Symmetric Encryption: Semantic Security, CPA-Security, Message Integrity and Message Authentication Codes (MACs), Authenticated Encryption, Differential Cryptanalysis, Linear Cryptanalysis.	
NUMBER-THEORETIC CRYPTOGRAPHY	**(06 Hours)**
The Discrete Logarithm Problem, Diffie-Hellman Key Exchange and ElGamal Encryption, Random Self-Reducibility and The Naor-Reingold PRF, Factoring and The RSA Assumption, Trapdoor Permutations and Digital Signatures, The Random Oracle Model.	
ELLIPTIC-CURVE CRYPTOGRAPHY	**(07 Hours)**
Generic Algorithms for Discrete Logarithm, Elliptic-Curve Cryptography: Notation, Definitions, and Constructions, Introduction to Pairing-Based Cryptography, 3-Party Non-Interactive Key-Exchange from Pairings, Short Signatures From Pairings, Identity-Based Encryption from Pairings.	
ENCRYPTED DATA PROCESSING	**(06 Hours)**
Homomorphic Signatures, Partial Homomorphic Encryption, Somewhat Homomorphic Encryption, Fully Homomorphic Encryption, Dual Regev Encryption, Attribute-Based Encryption.	
ZERO-KNOWLEDGE PROOF	**(06 Hours)**
Zero-Knowledge Proof System, Interactive Proof Systems, Zero-Knowledge Proof Systems and The Simulation Paradigm, Zero-Knowledge Proofs for NP, Proofs of Knowledge, Sigma Protocols: Schnorr Signatures and Chaum-Pedersen Proofs, The Fiat-Shamir Heuristic, Differential Privacy.	
MULTI-PARTY COMPUTATION SYSTEMS	**(04 Hours)**
Secure Multi-Party Computation, Oblivious Transfer Protocols, Yao's Garbled Circuits, Shamir Secret Sharing, Computing on Secret-Shared Data, SMPC in the Preprocessing Model: OT Correlations and Beaver Triples.	
LATTICE-BASED CRYPTOGRAPHY	**(06 Hours)**
Overview of Post-Quantum Cryptography, Introduction to Lattice-Based Cryptography, The Short Integer Solutions (SIS) Problem, Lattice Trapdoors, and Lattice-Based Signatures, The Learning With Errors (LWE) Problem, Regev's Public-Key Encryption Scheme from LWE.	
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**

(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)

BOOKS RECOMMENDED

1. Boneh, Dan, and Victor Shoup. "A graduate course in applied cryptography." Recuperado de https://crypto. stanford. edu/~ dabo/cryptobook/BonehShoup_0_4. pdf (2017).
2. Katz, Jonathan, and Yehuda Lindell. "Introduction to modern cryptography.", CRC press, (2020).
3. Goldreich, Oded. "Foundations of cryptography: volume 1 basic tools", Cambridge University Press, (2009).
4. Goldreich, Oded. "Foundations of cryptography: volume 2 basic applications", Cambridge University Press, (2009).
5. Bellare, Mihir, and Phillip Rogaway. "Introduction to modern cryptography." ,UCSD CSE 207 (2005).

Course Outcomes **At the end of the course, students will**	
CO1	be able to define advanced cryptography terminologies.
CO2	be able to apply various security models while designing applications and different security mechanisms to provide different security services that protect against security attacks.
CO3	be able to analyze different security models and protocols.
CO4	be able to evaluate encrypted data using encrypted data processing techniques.
CO5	be able to design, build, and deploy secure applications.

M. Tech. – I (CSE) ISP Semester – II	L	T	P	C
CSIS138: SECURITY PROTOCOLS (CORE ELECTIVE-3 OR 4)	3	0	2	4

Course Objective	
1	to understand concepts of security protocols and its analysis.
2	to understand how applications can communicate securely and what tools and protocols exist in order to offer different levels of security.
3	to get knowledge and the ability to critically analyze and design secure networks, applications and systems.
4	to give hands-on experience in using automated tools and formal techniques to analyze and evaluate cryptographic protocols and other security mechanisms.
5	to analyze various existing protocols in terms of the goals.

INTRODUCTION TO SECURITY PROTOCOLS	**(04 Hours)**
Introduction to Computer Security, Security Protocols, Security Analysis	
TRANSPORT LAYER SECURITY	**(05 Hours)**
Overview of SSL/TLS, Creating An Abstract Model, Coding Up in Murphi, Specification and Verification of Security Properties.	
KEY EXCHANGE PROTOCOLS	**(04 Hours)**
Key Management, Kerberos, Public-Key infrastructure, Security Properties and Attacks on Them, Needham-Schroeder Lowe Protocol, Diffie-Hellman Key Exchange, IPSec, Ike.	
CONTRACT-SIGNING PROTOCOLS	**(05 Hours)**
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.	
PASSWORD AUTHENTICATION	**(04 Hours)**
Hashed Password Files and Salt, Web Authentication Issues: Sniffing, Phishing, Spyware, Password-Authenticated Key Exchange Protocols.	
PROBABILISTIC MODEL CHECKING	**(05 Hours)**
Crowds System, Probabilistic Notions of Anonymity, Markov Chains, Prism, PCTL Logic, Probabilistic Fair Exchange.	
PROTOCOL VERIFICATION BY THE INDUCTIVE METHOD	**(04 Hours)**
Protocol Analysis Using Theorem Proving, Inductive Proofs, Isabelle Theorem Prover, Verifying the Secure Electronic Transactions (Set) Protocols Using Isabelle.	
PROBABILISTIC CONTRACT SIGNING	**(04 Hours)**
Rabin's Beacon, Rabin's Contract Signing Protocol, BGMR Probabilistic Contract Signing, formal Model for the BGMR Protocol.	
GAME-BASED VERIFICATION OF FAIR EXCHANGE PROTOCOLS	**(04 Hours)**
The Problem of Fair Exchange, Protocol As A Game Tree, Alternating Transition Systems, Alternating-Time Temporal Logic, Mocha Model Checker.	
OTHER SECURITY PROTOCOLS	**(06 Hours)**
Yahalom Protocol: Secrecy, Authentication, Non-Repudiation, Anonymity; Dolev-Yao Threat Model, Needham- Schroeder Public-Key Protocol and Its Security Analysis. Wireless Networking Protocol, Logic for Computer Security Protocols: Floyd-Hoare Logic of Programs, Ban Logic, Compositional Logic for Proving Security Properties of Protocols, Probabilistic Polynomial-Time Process Calculus for	

Security Protocol Analysis.	
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

BOOKS RECOMMENDED

1. Peter Ryan, Steve Schneider, Michael Goldsmith, Gavin Lowe, Bill Roscoe, " Modelling & Analysis of Security Protocols", Addison Wesley, 2000.
2. Stephen W. Mancini, "Automating Security Protocol Analysis", Biblioscholar, 2012.
3. Ulysess Black, "Internet Security Protocols**:** Protecting IP Traffic**",** Prentice Hall PTR; 1st edition, ISBN-10: 0130142492, ISBN-13: 978-0130142498, 2000.
4. Giampaolo Bella, "formal Correctness of Security Protocols", Springer, 2007.
5. Dinesh Goyal, S. Balamurugan, Sheng-Lung Peng, O.P. Verma, "Design and Analysis of Security Protocol for Communication, Scrivener Publishing, 2020.

Course Outcomes At the end of the course, students will	
CO1	be able to understand different authentication techniques, key exchange protocols and security issues while designing the protocols.
CO2	be able to get a hands-on exposure to the principles and techniques used in security systems, as well as designing security protocols.
CO3	be able to analyse the security protocols against different attacks.
CO4	be able to evaluate vulnerabilities in the security systems
CO5	be able to design a key agreement or key transport or key establishment protocol satisfying various security goals.

M. Tech. – I (CSE) ISP Semester – II	L	T	P	C
CSIS140: HARDWARE SECURITY (CORE ELECTIVE-3 OR 4)	3	0	2	4

Course Objective	
1	to understand hardware based security primitives and protocols
2	to identify security threats for modern hardware design and practices
3	to understand different defense techniques to secure hardware
4	to explore practical real world case studies to design secure hardware

INTRODUCTION TO HARDWARE SECURITY	**(04 Hours)**
Overview and Layers of Computing System, Hardware Trust and Security, Attacks, Vulnerabilities, and Countermeasures, Conflict Between Security and Test/Debug	
HARDWARE TROJANS	**(07 Hours)**
Introduction, SoC Design Flow, Hardware Trojans, Hardware Trojans in FPGA Designs, Hardware Trojans Taxonomy, Trust Benchmarks, Countermeasures Against Hardware Trojans, Hands-on Experiment: Hardware Trojan Attacks	
HARDWARE IP PIRACY AND REVERSE ENGINEERING	**(07 Hours)**
Introduction, Hardware intellectual Property (IP), Security Issues in IP-Based SoC Design- Hardware Trojan Attacks, IP Piracy and Overproduction, Reverse Engineering, Security Issues in FPGA- FPGA Preliminaries, Lifecycle of FPGA-Based System, Hands-on Experiment: Reverse Engineering and Tampering	
SIDE-CHANNEL ATTACKS	**(08 Hours)**
Taxonomy of Side-Channel Attacks, Power Analysis Attacks-, Higher-order Side-Channel Attacks, Electromagnetic (EM) Side-Channel Attacks, Fault injection Attacks, Timing Attacks, Covert Channels.	
PCB SECURITY	**(08 Hours)**
PCB Security Challenges, Attacks on PCB, PCB Authentication, Sources of PCB Signature, Signature Assessment Metric, PCB integrity Validation.	
HARDWARE SECURITY PRIMITIVES	**(07 Hours)**
Physically Unclonable Function, True Random Number Generator, Design for Anti-Counterfeit, Hardware Obfuscation, Use of Obfuscation Against Trojan Attacks	
ADVANCED TOPICS	**(04 Hours)**
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

BOOKS RECOMMENDED

1. Ahmad-Reza Sadeghi, David Naccache, " Towards Hardware-intrinsic Security", Springer, 2010.
2. Debdeep Mukhopadhyay and Rajat Subhra Chakraborty, " Hardware Security: Design, Threats, and Safeguards", CRC Press.
3. Stefan Mangard, Elisabeth Oswald, Thomas Popp, "Power analysis attacks - revealing the secrets of smart cards", Springer 2007.
4. Rebeiro Chester, Mukhopadhyay Debdeep, Bhattacharya Sarani, " Timing Channels in Cryptography A Micro-Architectural Perspective", Springer. 2015.
5. Ted Huffmire et al, "Handbook of FPGA Design Security" , Springer. 2014.

Course Outcomes **At the end of the course, students will**	
CO1	be able to understand hardware security concepts
CO2	be able to assess the security of different hardware designs
CO3	be able to apply different hardware security techniques for modern hardware designs
CO4	be able to implement and evaluate different hardware security techniques.
CO5	be able to design secure hardware systems

M. Tech. – I (CSE) ISP Semester – I	L	T	P	C
CSIS172: SOCIAL NETWORKS (INSTITUTE ELECTIVE)	**3**	**0**	**0**	**3**

Course Objective	
1	To understand the social network models, representation and analytics.
2	To identify the unique challenges involved in social network research.
3	To apply techniques for social network representation and analytics for real-word scenarios.
4	To analyse and evaluate the social network research solutions for real-world scenarios.

INTRODUCTION	**(09 Hours)**
Introduction To Social Networks: Networks as Information Maps, Networks as Conduits, Connections, Propinquity, Homophily	
SOCIAL NETWORK REPRESENTATION	**(18 Hours)**
Social Network Analysis:Mathematical Foundations, Data Collection, Data Management, Visualization, Centrality, Subgroups, Cliques, Clusters, Dyads and Triads, Density, Structural Holes, Weak Ties, Centrality, The Small World, Circles, and Communities, Multiplicity, Structural Similarity and Structural Equivalence	
SOCIAL NETWORK ANALYSIS	**(09 Hours)**
Social Networks and Diffusion: Influence and Decision-Making, Epidemiology and Network Diffusion, Tipping Points and Thresholds	
TOOLS AND CASE STUDIES	**(09 Hours)**
Social Network Tools and Case Studies	
	(Total Contact Time: 45 Hours)

BOOKS RECOMMENDED

1. Borgatti SP, Everett MG, Johnson JC, “Analyzing Social Networks”, London, Sage Publication, 2013.
2. Kadushin C., “Understanding Social Networks: Theories, Concepts and Findings”, Oxford University Press, 2012.
3. Piet A.M. Kommers, Pedro Isaias, Tomayess Issa, “Perspectives on Social Media: A Yearbook”, Taylor and Francis, 2014.
4. Newman Mark, “Networks: An Introduction”, Oxford university press, 2018.
5. Brath Richard, David Jonker, "Graph analysis and visualization: Discovering Business Opportunity in Linked Data", John Wiley & Sons, 2015.

Course Outcomes **At the end of the course, students will**	
CO1	have the knowledge of various social network representation, visualization and analytics tools and techniques.
CO2	be able to apply tools for social network data acquisition, management and analytics.
CO3	be able to analyse and evaluate the social network research solutions for real-world scenarios
CO4	be able to design the social network analytics solution for the complex real-world problem.

M. Tech. – I (CSE) ISP Semester – II	L	T	P	C
CSIS174: CYBER LAWS (INSTITUTE ELECTIVE)	3	0	0	4

Course Objective	
1	The course aims at acquainting the students with the basic concepts of Cyber Law and also puts those concepts in their practical perspective.
2	It also provides an elementary understanding of the authorities under IT Act as well as penalties and offences under IT Act.
3	It also covers overview of Intellectual Property Right and Trademark Related laws with respect to Cyber Space.
4	Student will get the knowledge about the E- Governance policies of India.

INTRODUCTION OF CYBER CRIMES & CYBER LAW	**(07 Hours)**
Understanding Cyber Crimes and Cyber Offences, Crime in context of Internet, Types of Crime in Internet, Crimes targeting Computers: Definition of Cyber Crime & Computer related Crimes, Constraint and Scope of Cyber Laws, Social Media and its Role in Cyber World, Fake News, Defamation, Online Advertising.	
PREVENTION OF CYBER CRIMES & IT ACT 2000	**(07 Hours)**
Prevention of Cyber Crimes & Frauds, Evolution of the IT Act 2000, Genesis and Necessity. Critical analysis & loopholes of The IT Act, 2000 in terms of cyber-crimes, Cyber Crimes: Freedom of speech in cyber space & human right issues.	
FEATURES OF IT ACT 2000 & AMENDMENTS	**(07 Hours)**
Salient features of the IT Act, 2000, Cyber Tribunal & Appellate Tribunal and other authorities under IT Act and their powers, Penalties & Offences under IT Act, Amendments under IT Act and Impact on other related Acts (Amendments): (a) Amendments to Indian Penal Code. (b) Amendments to Indian Evidence Act. (c) Amendments to Bankers Book Evidence Act. (d) Amendments to Reserve Bank of India Act.	
INDIAN PENAL LAW	**(06 Hours)**
Indian Penal Law and Cyber Crimes: (i) Fraud, (ii) Hacking, (iii) Mischief, Trespass (iv) Defamation (v) Stalking (vi) Spam, Issues of Internet Governance: (i) Freedom of Expression in Internet (ii) Issues of Censorship (iii) Hate Speech (iv) Sedition (v) Libel (vi) Subversion (vii) Privacy, Cyber Appellate Tribunal with Special Reference to the Cyber Regulation Appellate Tribunal (Procedures) Rules 2000.	
GLOBAL IT RULES & IPR	**(06 Hours)**
The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 and Corresponding International Legislation in US, UK and Europe, The Information Technology (Procedures and Safeguards for Blocking the access of Information by Public) Rules, 2009 and Corresponding International Legislation in US, UK and Europe, The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2009 and Corresponding International Legislation in US, UK and Europe, Intellectual Property Right (IPR).	
CYBER SPACE & E-GOVERNANCE IN INDIA	**(06 Hours)**
Cyber and Cyber Space with reference to Democracy and Sovereignty, Developments in Cyber law Jurisprudence, Role of law in Cyber World: Regulation of Cyber Space in India, Role of RBI and Legal Issues in case of e-commerce, E-Governance in India: Law, Policy, Practice.	
CYBERSPACE JURISDICTION	**(06 Hours)**
Cyberspace Jurisdiction (a) Jurisdiction issues under IT Act, 2000. (b) Traditional principals of Jurisdiction	

(c) Extra-terrestrial Jurisdiction (d) Case Laws on Cyber Space Jurisdiction (e) Taxation issues in Cyberspace.	
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

BOOKS RECOMMENDED

1. Vakul Sharma , "Information Technology Law and Practice- Cyber Laws and Laws Relating to E-Commerce", Universal Law Publishing - An imprint of LexisNexis.
2. Duggal Pavan , "Legal Framework on Electronic Commerce and Intellectual Property Rights in Cyberspace", Universal Law Publishing - An imprint of LexisNexis.
3. Yatindra Singh , "Cyber Laws: A Guide to Cyber Laws, Information Technology, Computer Software, Intellectual Property Rights, E-commerce, Taxation, Privacy, Etc. Along with Policies, Guidelines and Agreements", Universal Law Publishing
4. Santosh Kumar, "Cyber Laws & Cyber Crimes", WHITESMANN.
5. Akash Kamal Mishra , "Cyber Laws in India - Fathoming Your Lawful Perplex " , Notion Press, 2020.

Course Outcomes **At the end of the course, students will be able**	
CO1	Students will be able to understand the types of Crime in Internet, Crimes targeting Computers and Scope of Cyber Laws.
CO2	Students will be able to apply the cyber laws to relate the various evidences of cybercrimes.
CO3	Students will be able to analyze the various evidence of cybercrimes to be allied with the particular cyber law.
CO4	Students will be able to evaluate the particular intellectual property rights according to the cyber law.
CO5	Students will be able to design an application to counter the cybercrimes.

M. Tech. – I (CSE) ISP Semester – II	L	T	P	C
CSIS176: ETHICAL HACKING AND PENETRATION TESTING (INSTITUTE ELECTIVE)	**3**	**0**	**2**	**4**

Course Objective	
1	to describe the fundamental concepts of protecting a network from attacks.
2	to enumerate the techniques for collecting the network and the host information by a remote user.
3	to learn the techniques by which the adversary can discover and do mapping of systems, can orchestrate unauthorized manipulation of data, disable network systems or services and deny access to resources by legitimate users.
4	to analyse the techniques used by the adversary to detect the common vulnerabilities.
5	to apply the knowledge gained to protect the network as well as the host systems from the adversary attacks.

INTRODUCTION	**(04 Hours)**
Review of the Network Fundamentals, Network Topologies, Network Components, TCP/IP Networking Basics, TCP/IP Protocol Stack: DNS, SNMP, TCP, UDP, IP, ARP, RARP, ICMP protocols. Ethernet, Subnet Masking, Subnetting, Supernetting. Review of the Security Basics: Attributes, Mechanisms and Attacks Taxonomy. The CIA Traid. Threats, Vulnerabilities, Attacks	
NETWORK SECURITY CONCERNS	**(04 Hours)**
Network Security Concerns. Fundamental Network Security Threats. Types of Network Security Threats. Network Security Vulnerabilities, their types: Technological Vulnerabilities, Configuration Vulnerabilities, Security policy Vulnerabilities. Types of Network Security Attacks	
INTELLIGENCE (INT) GATHERING	**(09 Hours)**
Learning about the target, its business, its organizational structure, and its business partners. To output the list of company names, partner organization names, and DNS names, and the servers. The concepts of Search engines, Financial databases, Business reports. The use of WHOIS, RWHOIS, Domain name registries and registrars, Web archives and the corresponding open source tools for mining these data. Cloud reconnaissance.	
NETWORK FOOTPRINTING	**(09 Hours)**
Active & Passive Footprinting. Network and system footprinting. Tools for network footprinting. Using Search engines to find the tools. Mining the DNS host names, corresponding IP addresses, IP address ranges, Firewalls, Network maps. Use of search engines, social media, social engineering, the websites of the target organization. Using archive.org. Using Neo trace, *DNS Footprinting* and whois databases. Use of the contemporary tools (e.g. png, port scanners) for finding these information. Email footprinting. Email Tracking. Footprinting through Google tools. Using traceroute. Verification to confirm the validity of information collected in the prior phases. The countermeasures to prevent successful network footprinting.	
SCANNING & ENUMERATION	**(09 Hours)**
Scanning: goals and type, overall scanning tips, sniffing with tcpdump, network tracing, port scanning. OS fingerprinting, version scanning. Identify open ports. Web Service Review Tools: Identify web-based vulnerabilities. Network Vulnerability Scanning Tools: Identify infrastructure-related security issues. The illustrative tools are Nmap, ping, AngryIP, Nikto, OpenVAS, udp-proto-scanner, Netsparker, Nessus, Masscan, SQLMap, Nexpose, Burpsuite, Qualys, HCL AppScan, Amass, wpscan, Eyewitness, WebInspect, ZAP. Stealth Scanning: Scanning Beyond an IDS. Network diagram generation using typical tools viz. Network Topology Mapper, OpManager, LANState, Friendly	

Pinger. Proxy Servers, The Onion Routing. http tunneling. ssh tunneling. Anonymizers.	
EXPLOITATION	**(10 Hours)**
Network based exploitation: using tools such as Metasploit to compromise vulnerable systems, basics of pivoting, and pilfering. Detection of IP Spoofing. Common web vulnerabilities: Cross-site scripting, OS and Command injections, Buffer overflows, SQL injection, race conditions, and such other vulnerabilities scanning and exploitation techniques, including those in OWASP Top 25. Extracting information about the user names using email IDs, the list of default passwords used by the products used at the target, usernames using the SNMP protocol, user groups from Windows and the DNS zone transfer information. SuperScan. Route Analysis Tools. SNMP Enumeration. Reconnaissance Attacks and how to mitigate reconnaissance attacks.	
Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements will be changed every year and will be notified on Website.)	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

BOOKS RECOMMENDED

1. John Slavio, “Hacking: A Beginners’ Guide to Computer Hacking, Basic Security, And Penetration Testing”.
2. Yuri Diogenes, Dr. Erdal Ozkaya, “Cybersecurity – Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals”, 2nd Edition Kindle Edition, Packt Publishing; 2nd edition, 2019.
3. Hidaia Mahmood Alassouli, “Footprinting, Reconnaissance, Scanning and Enumeration Techniques of Computer Networks”, Blurb Publishers.
4. Robert Shimonski, “Cyber Reconnaissance, Surveillance and Defense 1st Edition, Kindle Edition, Syngress; 2014.
5. Sikorski, Michael, and Honig, Andrew, “Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software”, United States, No Starch Press, 2012.

ADDITIONAL BOOKS RECOMMENDED

1. Dafydd Stuttard and Marcus Pinto, “The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws”.

Course Outcomes **At the end of the course, students will**	
CO1	have a knowledge of the basic concepts of network, host, services and vulnerability gathering techniques employed by an attacker.
CO2	be able to use the tools for doing network footprinting including stealth scanning.
CO3	be able to analyze the installations for the vulnerabilities that could be exploited by an adversary.
CO4	be able to design secure system installations that can withstand adversarial attacks.
CO5	be able to extend the existing tools for network and systems protection.