Course structure for M.Tech in Cyber Security
Department of CSE, NIT Agartala

Semester	Subject	L	T	P	Credit	Class Hours Per week	Marks
1	1. Advanced Data Structures and Algorithms	3	1	0	4	4	100
	2. Mathematical Foundation of Computer Science	3	1	0	4	4	100
	3. Principles of Cryptography	3	1	0	4	4	100
	4. Elective-I * ***To be chosen from the list of electives.**	3	1	0	4	4	100
	5. Elective –II * ***To be chosen from the list of electives.**	3	1	0	4	4	100
	6. Laboratory - I (Advanced Data Structures and Algorithms)	0	0	2	2	3	100
	7. Laboratory - II (Cryptography)	0	0	2	2	3	100
	8. Seminar			1	1	2	100
	Total	15	5	5	25	28	800
2	1. Information Security & Risk Management	3	1	0	4	4	100
	2. Design of Secure Protocols	3	1	0	4	4	100
	3. Elective-III ***To be chosen from the list of electives.**	3	1	0	4	4	100
	4. Elective –IV ***To be chosen from the list of electives.**	3	1	0	4	4	100
	5. Laboratory-III (Cyber Security & Digital Forensic)	0	0	2	2	3	100
	6. Laboratory-IV ()	0	0	2	2	3	100
	7. Project Preliminary	0	0	3	3	6	100
	8. Comprehensive Viva			2	2	0	100
	Total	12	4	9	25	28	800

Semester	Subject	L	T	P	Cr.		Marks
3	Project and Thesis - 1 *	0	0	10	10	FULL	100
	Total	0	0	10	10		100
4	Project and Thesis - 2 *	0	0	20	20	FULL	300
	Total	0	0	20	20		300
	* For Project and Thesis - 1 & 2 Students may go for industrial or inter institutecollaboration, based Project work for 6 months to 1 year. The DPPC and concerned local guide may be empowered to recommend such provision. All existing academic rules of institute will prevail. The exact modalities may be recommended by DPPC.					Class Hours per week	

Cumulative credit of the course							
Semester-I		15	5	5	25	28	800
Semester -II		12	4	9	25	28	800
Semester -III		0	0	10	10	Full	100
Semester -IV		0	0	20	20	Full	300
Total		30	6	44	80		2000

S. No.	List of Elective Subjects	L	T	P	Cr.	Class Hours per week	Marks
1	Information Systems Control & Audit	4	0	0	4	4	100
2	Natural Language Processing	4	0	0	4	4	100
3	Soft computing	4	0	0	4	4	100
4	Data Mining	4	0	0	4	4	100
5	Secure Software Engineering	4	0	0	4	4	100
6	Advanced Computer Networks	4	0	0	4	4	100
7	Information Retrieval	4	0	0	4	4	100
8	Coding Theory	4	0	0	4	4	100
9	Cyber Crime, Cyber Laws & IPR	4	0	0	4	4	100
10	Data Hiding	4	0	0	4	4	100
11	Deep learning	4	0	0	4	4	100
12	Secure Coding	4	0	0	4	4	100
13	Social Network Analysis	4	0	0	4	4	100
14	Cyber Forensics, Audit & Investigation	4	0	0	4	4	100
15	Cloud and IoT Security	4	0	0	4	4	100
16	Big Data Analytics	4	0	0	4	4	100
17	Ethical Hacking	4	0	0	4	4	100
18	Wireless Network Security	4	0	0	4	4	100

Annexure - I

Detail Syllabus
for M. Tech in Cyber Security,
Department of CSE, NIT Agartala

Semester I

1.1 Advanced Data Structures and Algorithms	
L T P 3 ,1, 0: **4 Credits**	Prerequisites: *None*

Course Objectives:

1. The course is intended to provide the foundations of the practical implementation and usage of Algorithms and Data Structures.
2. One objective is to ensure that the student evolves into a competent programmer capable of designing and analyzing implementations of algorithms and data structures for different kinds of problems.
3. Another objective is to expose the student to the algorithm analysis techniques, to the theory of reductions, and to the classification of problems into complexity classes.

Detailed syllabus:

MODULE I

Introduction to advanced data structures, Fundamentals of the analysis of algorithms, Algorithms, Performance analysis- time complexity and space complexity, Asymptotic Notation-Big Oh, Omega and Theta notations, Complexity Analysis Examples. Data structures-Linear and nonlinear data structures, ADT concept, Linear List ADT, Recurrences: The substitution method, Recursive tree method, Masters Method, Probabilistic analysis, Amortized analysis, Randomized algorithms, Mathematical aspects and analysis of algorithms.

MODULE II

Divide and Conquer technique, Binary search tree, AVL-trees, red-black trees, B and B+-trees, Finding the minimum and maximum, Merge sort, Quick sort, Strassen's matrix multiplication. Splay Trees, Binomial Heaps, Fibonacci Heaps, Application of k-d tree (k-dimensional tree) in range searches and nearest neighbor searches.

MODULE III

Greedy algorithms: Introduction, Knapsack problem, Job sequencing with deadlines, Minimum cost spanning trees, Kruskal's algorithm, Prim's algorithm, Optimal storage on

tapes, Optimal merge pattern, Subset cover problem, Container loading or Bin packing problem.

MODULE IV

Dynamic algorithms: Introduction Dynamic algorithms, All pair shortest path, 0/1 knapsack, Travelling salesman problem, Coin Changing Problem, Matrix Chain Multiplication, Flow shop scheduling, Optimal binary search tree (OBST), Analysis of All problems, Introduction to NP-Hard And NP- Complete Problems

More algorithms: Dynamic programming, graph algorithms: DFS, BFS, topological sorting, shortest path algorithms, network flow problems.

MODULE IV

String Matching: The naïve string-matching algorithm, Rabin Karp algorithm, KnuthMorrisPratt algorithm (KMP), longest common subsequence (LCS), Fractional cascading, suffix trees, geometric algorithms.

References:

1. Introduction to algorithms: Cormen, Leiserson, Rivest and Stein (Main textbook)
2. Algorithm Design: Kleinberg and Tardos
3. Data structures and algorithm analysis in C++ (Java): Mark Weiss
4. Data structures and algorithms: Aho, Hopcroft and Ullman
5. S. Sahni, Data Structures, Algorithms, and Applications in C++, Silicon Press

Course Outcome (CO):

Course Outcome No.	Course Outcome
CO1	Basic ability to analyze algorithms and to determine algorithm correctness and timeEfficiency class.
CO2	Master a variety of advanced abstract data type (ADT) and data structures and theirimplementations.
CO3	Master different algorithm design techniques (brute-force, divide and conquer,greedy, etc.
CO4	Ability to apply and implement learned algorithm design techniques and datastructures to solve problem.

CO-PO Mapping: 1 - Slightly; 2 - Moderately; 3 – Substantially

CO	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1	1	1	2	1	2
CO2	1	2	2	2	2	1
CO3	2	2	2	2	2	2
CO4	3	3	1	3	3	3
Total	7	8	6	9	8	8
Attainment	2	2	2	2	2	2

1.2 Mathematical Foundation for Computer Science	
L T P 3 ,1, 0: **4 Credits**	Prerequisites: *None*

Course Objectives:

1. The basics of mathematical models used in information security.
2. The general understanding of cyber security relationship with numbers.
3. The security model and analyze them before being used in many commercial, industrial as well as web application.
4. The role of mathematics in a complex system such as the Internet.

Detailed syllabus:

MODULE – I: NUMBER THEORY DISCRETE MATHEMATICS
Definition - Divisibility - Greatest common divisor - Prime numbers - Fundamental theorem of arithmetic - Mersenne primes - Fermat numbers - Euclidean algorithm - Fermat‟s theorem - Euler totient function - Euler‟s theorem. Congruences: Definition - Basic properties of congruences - Residue classes - Chinese remainder theorem.

MODULE – II: DISCRETE MATHEMATICS
Algebraic Structures: Groups – Cyclic groups, Cosets, Modulo groups - Primitive roots - Discrete logarithms. Rings – Sub rings, ideals and quotient rings, Integral domains. Fields – Finite fields – GF(pn), GF(2n) - Classification - Structure of finite fields. Lattice, Lattice as Algebraic system, sub lattices, some special lattices.

MODULE – III: PROBABILITY THEORY
Introduction – Concepts of Probability - Conditional Probability - Baye‟s Theorem - Random Variables – discrete and continuous- central Limit Theorem-Stochastic ProcessMarkov Chain Bayesian methods of estimation. Random Processes: general concepts, power spectrum, discrete-time processes, random walks and other applications, Markov chains, transition probabilities.

MODULE - IV: CODING THEORY
Coding Theory: Introduction - Basic concepts: codes, minimum distance, equivalence of codes, Linear codes - Linear codes - Generator matrices and parity-check matrices - Syndrome decoding – Hamming codes – Hadamard Code - Goppa codes.

MODULE - V: PSEUDORANDOM NUMBER GENERATION
Introduction and examples - Indistinguishability of Probability Distributions - Next Bit Predictors - The BlumBlum-Shub Generator – Security of the BBS Generator.

TEXT/ REFERENCE BOOKS:

1. D. S. Malik, J. Mordeson, M. K. Sen, "Fundamentals of Abstract Algebra, Tata McGraw Hill. 2. P. K. Saikia, "Linear Algebra", Pearson Education.
2. Niven, H.S. Zuckerman and H. L. Montgomery, "An Introduction to the Theory of Numbers", John Wiley and Sons,.
3. D P Bersekas and J N Tsitsiklis, "Introduction to Probability", Athena Scientific.
4. C.L. Liu, Elements of Discrete mathematics", McGraw Hill,.
5. Leigh Metcalf, William Casey, "Cybersecurity and Applied Mathematics", Syngress Publisher.
6. Chuck Easttom, "Modern Cryptography: Applied Mathematics for Encryption and Information Security".

Course Outcome (CO):

Course Outcome No.	Course Outcome
CO1	Effectively express the concepts and results of Number Theory.
CO2	Understand basic concepts of various algebraic structures and theorems for designing security algorithm.
CO3	Understand coding theory which will be useful for data compression, information hiding.
CO4	Illustrate various pseudorandom number generation used for designing security protocols and for its analysis.

CO-PO Mapping: 1 - Slightly; 2 - Moderately; 3 – Substantially

CO	PO1	PO2	PO3	PO4	PO5	PO6
CO1	3	1	1			1
CO2	2	3	3	1	1	1
CO3		1	1	2	1	1
CO4	1		2	2	2	1
Total	6	5	7	5	4	4
Attainment	2	1	2	1	1	1

1.3 Principles of Cryptography	
L T P 3 ,1, 0: **4 Credits**	Prerequisites: *None*

Course Objectives

This course provides an in-depth idea to cryptography, its mathematical foundations, and its relation to security. It covers classical cryptosystems, private-key cryptosystems (including DES and AES), hashing and public-key cryptosystems (including RSA). The course also provides an inside to data integrity and authentication.

Course Content

MODULE I:

Algebra: Group, cyclic group, cyclic subgroup, field, probability. Number Theory: Fermat's theorem, Cauchy 's theorem, Chinese remainder theorem, primality testing algorithm, Euclid's algorithm for integers, quadratic residues etc..

MODULE II:

Classical cryptosystems and their cryptanalysis, Model of secure communication, Security services, Overview of attacks, X.800 Security Architecture for Open System Interconnection (OSI), and cryptanalysis, Shannon perfect secrecy, OTP, Pseudo random bit generators, stream ciphers and RC4.

MODULE III:

Block ciphers: Modes of operation, DES and its variants, AES, linear and differential cryptanalysis.

MODULE IV:

One-way function , trapdoor one-way function, Public key cryptography, RSA cryptosystem, Rabin cryptosystem, Diffie-Hellman key exchange algorithm, Elgamal Cryptosystem.

MODULE V:

Cryptographic hash functions, secure hash algorithm, Message authentication, Zero knowledge proofs, digital signature, RSA digital signature, Elgamal digital signature, Kerberos, X.509 authentication service, PKI Public Key Cryptography standard (PKCS), PKI, Digital Certificates, and Key management techniques.

References:

1. B. S. Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C.
2. Behrouz A. Forouzan and Debdeep Mukhopadhyay, Cryptography and Network Security, Tata McGraw Hill.

3. Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, ''Handbook of Applied Cryptography'', CRC Press.
4. Jonathan Katz and Yehuda Lindell, Introduction to Modern Cryptography, Chapman and Hall/CRC Press.
5. Oded Goldreich, The Foundations of Cryptography, Volume 1 and Volume 2, Cambridge University Press.

Course Outcomes

CO1	Students will be able to understand the classical and modern concepts related to cryptography and cryptanalysis.
CO2	Students will be able to know the mathematical support for cryptography and learn methods for modern cryptography techniques under the category of stream and block cipher.
CO3	Students will be able to analyze and implement of some of the prominent techniques for symmetric-key encryption schemes like DES, AES etc..
CO4	Students will be able to describe and implement of some of the prominent techniques for public-key cryptosystems and digital signature schemes (e.g., Rabin, RSA, ElGamal, DSA)
CO5	Students will be able to understand the inner workings of Authentication schemes and how to correctly use them in real-world applications.
CO6	Students will be able to explain the notions of public-key infrastructure and digital signatures, and sketch their formal security definitions.

CO-PO Mapping: 1 - Slightly; 2 - Moderately; 3 – Substantially

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1	1	--	--	--	--
CO2	2	3	2	2	2	2
CO3	2	3	2	2	2	2
CO4	2	3	2	2	3	2
CO5	3	3	3	2	3	2
CO6	3	3	3	2	3	2
Total	11	16	12	10	13	10
Average	1.8	2.6	2	1.6	2.1	1.6
Eq. Average Attainment	2	3	2	2	2	2

Semester II

2.1 Information Security & Risk Management	
L T P 4 , 0 , 0 : **4 Credits**	Prerequisites: *None*

Objective:

To understand and development of concepts required for risk-based planning and risk management of computer and information systems.

Detailed Syllabus:

Module I:

An Introduction to Risk Management: Introduction to the Theories of Risk Management; The Changing Environment; The Art of Managing Risks.

Module II:

The Threat Assessment Process: Threat Assessment and its Input to Risk Assessment; Threat Assessment Method; Example, Threat Assessment.

Module III:

Vulnerability Issues: Operating System Vulnerabilities; Application Vulnerabilities; Public Domain or Commercial Off-the-Shelf Software; Connectivity and Dependence; Vulnerability assessment for natural disaster, technological hazards, and terrorist threats; implications for emergency response, vulnerability of critical infrastructures.

Module IV:

The Risk Process: What is Risk Assessment? Risk Analysis; Who is Responsible? Tools and Types of Risk Assessment: Qualitative and Quantitative risk Assessment; Policies, Procedures, Plans, and Processes of Risk Management; Tools and Techniques; Integrated Risk Management; Future Directions: The Future of the Risk Management.

Text Books/References:

1. Malcolm Harkins, Managing Risk and Information Security, Apress.
2. Daniel Minoli, Information Technology Risk Management in Enterprise Environments, Wiley.

Course Outcomes (CO):

CO No.	Course Outcome
CO1	Understand risk-planning & risk management of computer & information systems.
CO2	Apply vulnerability assessment for natural disaster
CO3	Analyzing the implications of emergency response
CO4	Design methods for risk mitigation for infrastructure

CO-PO Mapping:

CO	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1		1	1	1	1
CO2	2		1	2		2
CO3	1			1		1
CO4	2		2	2	1	2
Eq. Avg. Attainment	2	0	1	2	1	2

2.2 Design of Secure Protocols	
L T P 4 , 0 , 0 : **4 Credits**	Prerequisites: *None*

Detailed Syllabus:

Module I:

One-Way Functions, Pseudorandom Generators, Hash functions, Block ciphers, Stream Ciphers, Access Control Methods, Message Authentication and Digital Signatures.

Module II:

Vulnerabilities and Security Challenges of Wireless networks, Trust Assumptions, Adversary models and Protocols, Attacks against naming and addressing in the Internet, Security protocols for address resolution and address auto configuration.

Module III:

Security for global IP mobility, IP Security (IP Sec) protocol, Key Establishment and Revocation Protocols in Sensor Networks, Secure Neighbor Discovery, Secure routing protocols in multi-hop wireless networks, Provable Security for Ad-hoc Network routing protocols

Module IV:

Privacy preserving routing in Ad-hoc Networks, Location privacy in vehicular Ad-hoc networks, Secure protocols for behavior enforcement Game theoretic model of packet forwarding.

Text Books/References:

1. L. Buttyan, J. P. Hubaux, "Security and Cooperation in Wireless Networks", Cambridge University Press.
2. O. Goldrich,"Foundation of Cryptography-Vol.1 & Vol.2", Cambridge University Press.
3. James Kempf, "Wireless Internet Security: Architecture and Protocols", Cambridge University Press.

Course Outcomes (CO):

CO Number	Course Outcome
CO1	Design adversary models and protocols.
CO2	Analyze Secure protocols for global IP mobility
CO3	Develop cryptographic/authentication algorithms
CO4	Identify security threats in Advanced Wireless networks.

CO-PO Mapping:

CO	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1	1	1	1	1	
CO2		1	2	2	1	1
CO3	1	2	2	2	2	1
CO4	1	1	1	2	1	1
Total	3	4	6	7	5	3
Eq. Avg. Attainment	1	1	2	2	1	1

Detailed Syllabus of Electives

1. Information Systems Control & Audit	
L T P 3 ,1, 0: **4 Credits**	Prerequisites: *None*

Course Objectives:

1. To understand the foundations of information systems auditing
2. To understand the management, application control framework
3. To understand about the evidence collection and evidence evaluation process

Detailed syllabus:

MODULE - I
Overview of Information System Auditing, Effect of Computers on Internal Controls, Effects of Computers on Auditing, Foundations of information Systems Auditing, Conducting an Information Systems Audit. The management Control Framework-I: Introduction, Evaluating the planning Function, Evaluating the Leading Function, Evaluating the Controlling Function, Systems Development Management Controls, Approaches to Auditing Systems Development, Normative Models of the Systems Development Process, Evaluating the Major phases in the Systems Development Process, Programming Management Controls, Data Resource Management Controls.

MODULE - II
The Management Control Framework-II: Security Management Controls, Operations management Controls Quality assurance Management Controls. The Application Control Framework-I: Boundary Controls, Input Controls, Communication Controls.

MODULE -III
The Application Control Framework-II: Processing Controls, Database Controls, output Controls.

MODULE - IV
Evidence Collection: Audit Software, Code Review, Test Data, and Code Comparison, Concurrent Auditing techniques, Interviews, Questionnaires, and Control Flowcharts. Performance Management tools.

MODULE -V
Evidence Evaluation: Evaluating Asset Safeguarding and Data Integrity, Evaluating System Effectiveness, Evaluating System Efficiency.

Practice study: CISA examination questions.

REFERENCE BOOKS:

1. Ron Weber, Information Systems Control and Audit, Pearson Education.
2. John B. Kramerk, The CISA Prep Guide, Wiley Publications.
3. Information Systems Control and Audit, BOS, Institute of Chartered Accountants of India, New Delhi.
4. Jalote : Software Project Management in Practice, Pearson Education.

Course Outcome (CO):

Course Outcome No.	Course Outcome
CO1	Ability to recognize the propensity of errors and remedies in processes involving Information Technology.
CO2	A consummate knowledge of risks and controls in IT operations in Industry.
CO3	An ability to provide protective IT security guidelines for various types of Industries.
CO4	The necessary wherewithal to become an IS Auditor and/or Security specialist eventually.
CO5	Evaluate asset safeguarding and data integrity, system effectiveness and system Efficiency.

CO-PO Mapping:

1 - Slightly; 2 - Moderately; 3 – Substantially

CO	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1	1	2	2		1
CO2		1	2	2	1	
CO3		2	1	2	2	1
CO4	1	1	2	1	2	1
CO5	1		2	1	1	1
Total	3	5	9	8	6	4
Eq. Avg. Attainment	1	1	2	2	1	1

2. Natural Language Processing	
L T P 4 , 0 , 0 : **4 Credits**	Prerequisites: *None*

Course Objective:

1. Teach students the leading trends and systems in natural language processing.
2. Make them understand the concepts of morphology, syntax, semantics, and pragmatics of the language and that they are able to give the appropriate examples that will illustrate the mentioned concepts in the syllabus.
3. Teach them to recognize the significance of pragmatics for natural language understanding.
4. Enable students to be capable to describe the application based on natural language processing and to show the points of syntactic, semantic and pragmatic processing.

Detailed syllabus:

MODULE I

Sound: Biology of Speech Processing; Place and Manner of Articulation; Word Boundary Detection; Argmax based computations; HMM and Speech Recognition.

MODULE II

Words and Word Forms : Morphology fundamentals; Morphological Diversity of Indian Languages; Morphology Paradigms; Finite State Machine Based Morphology; Automatic Morphology Learning; Shallow Parsing; Named Entities; Maximum Entropy Models; Random Fields.

MODULE III

Structures : Theories of Parsing, Parsing Algorithms; Robust and Scalable Parsing on Noisy Text as in Web documents; Hybrid of Rule Based and Probabilistic Parsing; Scope Ambiguity and Attachment Ambiguity resolution.

MODULE IV

Meaning and pragmatics: Lexical Knowledge Networks, Wordnet Theory; Indian Language Wordnets and Multilingual Dictionaries; Semantic Roles; Word Sense Disambiguation; WSD and Multilinguality; Metaphors; Coreferences. Discourse, Dialogue and Conversational agents, Natural Language Generation, Machine Translation.

MODULE V

Web 2.0 Applications: Sentiment Analysis; Text Entailment; Robust and Scalable Machine Translation; Question Answering in Multilingual Setting; Cross Lingual Information Retrieval.

References:

1. Speech and Language Processing by Daniel Jurafsky, James H. Martin, Second Edition, Prentice Hall
2. James Allen, "Natural Language Understanding", 2/E, Addison-Wesley, 1994
3. Foundations of Statistical Natural Language Processing by Christopher D. Manning, Hinrich Schutze, MIT Press.
4. Statistical Language Learning by Charniack, Eugene, MIT Press, 1993.
5. The Handbook of Computational Linguistics and Natural Language Processing, Alexander Clark, Chris Fox, Shalom Lappin.
6. Steven Bird, Natural Language Processing with Python, 1st Edition, O'Reilly, 2009.

Course Outcome (CO):

CO No	Course Outcome
CO1	Understand the fundamental concept of NLP, Regular Expression, Finite State Automata along with the concept and application of word tokenization, normalization, sentence segmentation, word extraction, spell checking in the contextof NLP.
CO2	Understand the concept of Morphology such as Inflectional and Derivational Morphology and different morphological parsing techniques and scope of ambiguity and it's resolution.
CO3	Understand the concepts of pragmatics, lexical semantics, lexical dictionary such as WordNet, lexical computational semantics, distributional word similarity and concepts related to the field of Information Retrieval in the context of NLP.
CO4	Understand the concepts of Semantic Roles; Word Sense Disambiguation; Multilinguality; Metaphors; Coreferences. Discourse, Dialogue and Conversational agents, Natural Language Generation, Machine Translation.
CO5	Understand the concepts related to language modeling with introduction to N-grams, chain rule, smoothing, spelling and word prediction and their evaluation along with the concept of Markov chain, HMM, Forward and Viterbi algorithm, POS tagging.
CO6	Describe and apply concepts of discourse machine translation, summarization and question answering to solve problems in NLP.

CO-PO Mapping (Rate on a scale of 1 to 3):

CO	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1	1	1	1	1	1
CO2	2	2	2	2	1	2
CO3	2	2	3	2	1	3
CO4	2	3	3	3	3	3
CO5	3	3	3	3	3	3
CO6	3	3	3	3	3	3
Total	13	14	15	14	12	15
Average	2.16	2.3	2.5	2.3	2	2.5
Eq. Average Attainment	2	2	3	2	2	3

3. Soft Computing	
L T P 4 , 0 , 0 : **4 Credits**	Prerequisites: *None*

Course Objectives:

1. To develop students' skill in neuro-fuzzy engines to handle machine learning in presence of uncertainty.
2. To provide solutions to real world problems with approximate reasoning using fuzzy logic.
3. To instill the scope of optimization in engineering design using evolutionary computation.
4. To demonstrate the scope of the subject in all aspects of science, humanities, and engineering.
5. To emphasize on the necessity of soft techniques in engineering industry, where mathematically hard techniques are difficult to realize in absence of sufficient data.

Detailed syllabus:

MODULE I

Introduction to Fuzzy sets, Fuzzy t- and s- norms, projection, cylindrical extension, Fuzzy relations, Implication relations, Fuzzy relational equations, Possibilistic reasoning, Fuzzy pattern recognition, Introduction to Fuzzy control and Fuzzy databases.

MODULE II

Boltzmann machine and Mean field learning-Combinational optimization problems using recurrent Neural network. Competitive Learning, Self-organizing maps, Growing cell structure, Principal component analysis.

MODULE III

Genetic Algorithm: Binary and real codes, Genetic programming, Particle swarm optimization, Differential Evolution, Bacterial Foraging

MODULE IV

Hybridization of neuro-fuzzy, neuro-GA, neuro-swarm, neuro-evolution algorithms. Applications in Pattern Recognition, Robotics, and Image Processing.

MODULE V

Belief Networks: Pearl's Model for Distributed Approach of Belief Propagation and Revision in a causal network, Concepts of D-separation, Bayesian Belief Networks, Dempster-Shafer theory for Orthogonal summation of Beliefs, Data Fusion techniques, Uncertainty management using Belief Networks.

MODULE VI

Visual Perception: Marr's 2- and 1/2-Dimensional Vision, 3-D Vision, Camera Model, Perspective Projection Geometry, Inverse Perspective Projection Geometry, 3D Reconstruction from 2D Images by Kalman Filter and other Prediction Algorithms.

MODULE VII

Advanced Models of Reasoning: Soundness and Completeness issues of Resolution based Proof procedures in propositional and predicate logic, Herbrand's theorem and Lifting Lemma, Herbrand interpretation, Temporal Logic, Reasoning with Space and Time, Distributed Models of Reasoning using Petri Nets, and other graph theoretic approaches.

Text / References Books:

1. Computational Intelligence: Principles, Techniques, and Applications by A. Konar, Springer 2005
2. Computational Intelligence by A. P. Engelbrecht
3. Artificial Intelligence and Soft Computing: Behavioral and Cognitive Modeling of the Human Brain by A. Konar, CRC Press, 2018.
4. Multi-Agent Coordination: A Reinforcement Learning Approach by A. K. Sadhu and A. Konar, Wiley- IEEE Press, 2021.
5. D. E. Goldberg, Genetic Algorithms in Search Optimization and Machine Learning, Addison Wesley,3rd edition.
6. S. Haykin, Neural Networks: A comprehensive foundation, Pearson, 1999.

Course Outcomes:

CO1: Develops students' skill in neuro-fuzzy engines to handle machine learning in presence of uncertainty.
CO2: Provides solution to real world problems with approximate reasoning using fuzzy logic.
CO3: Instills the scope of optimization in engineering design using evolutionary computation.
CO4: Demonstrates the scope of the subject in all aspects of science, humanities and engineering.
CO5: Emphasizes the necessity of soft techniques in engineering industry, where mathematically hard techniques are difficult to realize in absence of sufficient data.

CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6
CO1	3	3	2	3	2	2
CO2	2	2	3	2	1	2
CO3	3	3	2	2	2	2
CO4	2	2	2	2	2	3
CO5	3	3	3	3	3	3
Total	13	13	12	12	10	12
Average	2.6	2.6	2.4	2.4	2	2.4

4. Data Mining	
L T P 3, 1, 0 : **4 Credits**	Prerequisites: *None*

Course Objective:

1. To understand Data Mining in Knowledge discovery process, and its applications.
2. To understand different data attribute types and apply different data preprocessing techniques.
3. To understand how to identify association among data objects by learning various association mining algorithms.
4. To understand the various classification & clustering techniques, their applications in different domains.
5. To learn various data visualization techniques for data analysis.

Detailed syllabus:

MODULE I
Introduction: Data Mining, Motivation, Application, Data Mining—On What Kind of Data? Data Mining Functionalities, Data Mining Task Primitives, Major Issues in Data Mining.
Data pre-processing: Attribute types, Similarity & Dissimilarity measures.

MODULE II
Data Preprocessing: Data Cleaning, Data Integration, Data Reduction, Data Transformation & Discretization.

MODULE III
Mining Frequent Patterns: Basic Algorithms, Association Rule Mining, Apriori Algorithm, FP tree growth Algorithm, Advanced Pattern Mining Techniques.

MODULE IV
Classification Techniques: Decision Tree, Bayes Classification, Bayesian Belief Networks, Support Vector Machines, Classification Evaluation Techniques, Classification Accuracy improvement Techniques.

MODULE V
Clustering Techniques: Partitioning algorithms, Hierarchical algorithms, Density-Based algorithms, Grid-Based algorithms, Evaluation of Clustering. Outlier Detection Techniques.
MODULE VI
Applications and Trends in Data Mining: Applications, Advanced Techniques, Web Mining, Web Content Mining, Structure Mining.

References Books:

5. J. Han and M. Kamber. Data Mining: Concepts and Techniques. 3rd Edition, Morgan Kaufman. Pang Ning Tan, Introduction to Data Mining, 2nd Edition, Pearson.
6. M. H. Dunham. Data Mining: Introductory and Advanced Topics. Pearson Education. Roiger & Geatz, Data Mining, Pearson Education
7. A.K.Pujari, Data Mining, University Press
8. I. H. Witten and E. Frank. Data Mining: Practical Machine Learning Tools and Techniques. Morgan Kaufmann.
9. D. Hand, H. Mannila and P. Smyth. Principles of Data Mining. Prentice, Hall.

Course Outcome (CO):

CO Number	Course Outcome
CO1	Students will be able to interpret the contribution of data mining inKnowledge discovery process.
CO2	Students will be able to identify different data attribute types andapply different data preprocessing techniques.
CO3	Students will be able to apply the link analysis and frequent item-set algorithms to identify the entities on the real-world data.
CO4	Students will be able to apply the various classification and clustering algorithms for supervised and unsupervised learningproblems.
CO5	Students will be able to apply various data visualization techniquesfor in-depth data analysis.
CO6	Students will be able to apply the advanced data mining techniquesand use the popular data mining tools.

CO-PO Mapping:

CO	PO1	PO2	PO3	PO4	PO5	PO6
CO1	2	2	2	1	1	--
CO2	2	2	2	--	--	--
CO3	3	2	3	1	--	--
CO4	3	3	3	1	2	1
CO5	3	3	3	1	2	1
CO6	3	3	3	1	3	2
Total	16	15	16	5	8	4
Average Attainment	2.7	2.5	2.7	0.8	1.3	0.7
Equivalent Average Attainment	3	3	3	1	1	1

5. Secure Software Engineering	
L T P 3, 1, 0 : **4 Credits**	Prerequisites: *None*

Detailed syllabus:

Modue I

Software assurance and software security, threats to software security, sources of software insecurity, benefits of detecting software security, managing secure software development.

Module II

Defining properties of secure software, how to influence the security properties of software, how to assert and specify desired security properties, Secure software Architecture and Design: Software security practices for architecture and design: Architectural risk analysis.

Module III

Software security knowledge for Architecture and Design: security principles, security guidelines, and attack patterns, secure design through threat modeling, Writing secure software code: Secure coding techniques, Secure Programming: Data validation.

Module IV

Secure Programming: Using Cryptography Securely, Creating a Software Security Programs. Secure Coding and Testing: code analysis- source code review, coding practices, static analysis, software security testing, security testing consideration through SDLC.

References Books:

1. Julia H Allen, Sean J Barnum, Robert J Ellison, Gary McGraw, Nancy R Mead, *Software Security Engineering: A Guide for Project Managers*, Addison Wesley,
2. Ross J Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd Edition, Wiley, 2008.
3. Howard, M. and LeBlanc, D., *Writing Secure Code*, 2nd Edition, Microsoft Press, 2003.
4. J. Han and M. Kamber. Data Mining: Concepts and Techniques. 3rd Edition, Morgan Kaufman. Pang Ning Tan, Introduction to Data Mining, 2nd Edition, Pearson.
5. M. H. Dunham. Data Mining: Introductory and Advanced Topics. Pearson Education. Roiger & Geatz, Data Mining, Pearson Education
6. A.K.Pujari, Data Mining, University Press
7. I. H. Witten and E. Frank. Data Mining: Practical Machine Learning Tools and Techniques. Morgan Kaufmann.
8. D. Hand, H. Mannila and P. Smyth. Principles of Data Mining. Prentice, Hall.

Course Outcome (CO):

CO Number	Course Outcome
CO1	Evaluate secure software engineering problems, including the specification, design, implementation, and testing of software systems.
CO2	Elicit, analyze and specify security requirements through SRS
CO3	Design and Plan software solutions to security problems using various paradigms
CO4	Model the secure software systems using Unified Modeling Language Sec(UMLSec)
CO5	Develop and apply testing strategies for Secure software applications

CO-PO Mapping:

CO	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1	1	2			
CO2	1	2	1	1		1
CO3	1	2	2	3	2	2
CO4	1	1	1		1	1
CO5	1	1	2	1	2	2
Total	5	7	8	5	5	6
Equivalent Average Attainment	1	1	2	1	1	1

6. Advanced Computer Networks	
L T P 3 ,1, 0: **4 Credits**	Prerequisites: *None*

Course Objectives: To give the students an understanding of the principles behind the latest advances in computer network technology, from IPv6 extending to pervasive and ubiquitous computing.

Detailed syllabus:

MODULE I

Opportunistic and Social Networks: Handling Spectrum Scarcity and Disruption, Architecture of Cognitive Radio Network (CRN) and Delay Tolerant Networks (DTN), Routing in Opportunistic Mobile and Social Networks, Multicasting, Single-node, Multiple-copy, and Single-copy model, Interest-based Data Dissemination, User Interest Profile, Multi-party data transmission, System Implementation, Quality-of-Service (QoS), QoS parameters, Metrics and classification, Network QoS parameters (bandwidth, delay, etc.), System QoS parameters (reliability, capacity, etc.), Task QoS parameters (memory, CPU usage, response time, etc.), Extension QoS parameters (reputation, security, etc.).

MODULE II

IoT Networks:Convergence of domains, Key technologies for IoT and its components, Multi-homing, Sensing, Actuation, Data Aggregation, IoT communication patterns, IoT data and its impact on communication, Characteristics of IoT networks, Protocols for IoT, NFC (Near field communication), Tactile Internet, Caching, Edge computing, Inter-dependencies, SoA, Gateways, Comparison between IoT and Web, Complexity of IoT networks, Scalability, Protocol classification, MQTT, SMQTT, CoAP, XMPP, AMQP, Wireless HART protocol and layered architecture, HART network manager, HART vs ZigBee, Cross layer QoS parameters.

MODULE III

Software Defined Networks (SDN):Network Function Virtualization (NFV), Unicast and multicast routing, Fundamental graph algorithms, Modern protocols for content delivery, Video delivery using HTTP, HTTP Live Streaming, DASH, Content Delivery Networks (CDN), TVOD and SVOD,

MODULE IV

Architecting a content distribution system over IP-based networks, CDN topologies, Edge-Caching, Streaming-Splitting, Pure-Play, Operator, Satellite, Hybrid, Computer hosting and orchestration for dedicated appliances and virtualization, Robust synchronization of absolute and difference clocks, Precision time protocol, Clock synchronization in SDN, ReversePTP scheme.

REFERENCE BOOKS:

1. Jie Wu and Yunsheng Wang, Opportunistic Mobile Social Networks, CRC Press
2. James F. Kurose and Keith W. Ross, Computer Networking: A Top-down Approach Featuring the Internet, Addison-Wesley.
3. Huitema, C., Routing in the Internet, 2nd ed., Prentice-Hall.
4. Peterson and Davie, Computer Networks: A Systems Approach., Morgan Kaufmann.
5. Rajiv Ramaswami, Kumar N. Sivarajan, Galen H. Sasaki, Optical Networks: A Practical Perspective, Morgan Kaufmann.
6. Vijay Madisetti and Arshdeep Bahga, Internet of Things: A Hands-On- Approach,, ISBN:978 0996025515
7. Francis daCosta, Rethinking the Internet of Things: A Scalable Approach to Connecting Everything, Apress Publications,

Course Outcome (CO):

Course Outcome No.	Course Outcome
CO1	To understand the concepts behind Opportunistic, IoT and Software Defined Networking.
CO2	To identify different issues in Opportunistic, Social, IoT and SDN Networks.
CO3	To analyze various protocols proposed to handle issues related to Opportunistic, Social, IoT and SDN Networks.

CO-PO Mapping:

1 - Slightly; 2 - Moderately; 3 – Substantially

CO	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1	1		1	1	
CO2	1	2	2	2	1	1
CO3		1	2	2	1	1
Total	2	4	4	5	3	2
Eq. Average Attainment	1	1	1	2	1	1

7. Information Retrieval	
L T P 4 , 0 , 0 : **4 Credits**	Prerequisites: *None*

Course objective:

1. To understand fundamental concepts of Information retrieval systems.
2. To understand the knowledge of data structures and indexing methods in information retrieval Systems.
3. To learn the evaluation of different indexing techniques.
4. To learn and develop indexing systems for audio and visual documents.
5. To learn the concept of searching of webs.

Detailed Syllabus:

MODULE I

Basic Concepts of IR, Data Retrieval & Information Retrieval, IR system block diagram. Automatic Text Analysis, Luhn's ideas, Conflation Algorithm, Indexing and Index Term Weighing, Probabilistic Indexing, Automatic Classification, Measures of Association, Different Matching Coefficient, Classification Methods, Cluster Hypothesis. Clustering Algorithms, Single Pass Algorithm, Single Link Algorithm, Rochhio's Algorithm and Dendograms.

MODULE II

File Structures, Inverted file, Suffix trees & suffix arrays, Signature files, Ring Structure, IR Models, Basic concepts, Boolean Model, Vector Model, and Fuzzy Set Model. Search Strategies, Boolean search, serial search, and cluster based retrieval, Matching Function.

MODULE III

Performance Evaluation, Precision and recall, alternative measures reference collection (TREC Collection), Libraries & Bibliographical system, Online IR system, OPACs, Digital libraries , Architecture issues, document models, representation & access, Prototypes, projects & interfaces, standards.

MODULE IV

Taxonomy and Ontology: Creating domain specific ontology, Ontology life cycle Distributed and Parallel IR: Relationships between documents, Identify appropriate networked collections, multiple distributed collections, parallel IR, MIMD Architectures, Distributed IR, Collection Partitioning, Source Selection, and Query Processing.

MODULE V

Multimedia IR models & languages, data modelling, Techniques to represent audio and visual

document, query languages Indexing & searching, generic multimedia indexing approach, Query databases of multimedia documents, Display the results of multimedia searches, one dimensional time series, two dimensional color images, automatic feature extraction.

MODULE VI

Searching the Web, Challenges, Characterizing the Web, Search Engines, Browsing, Mata searchers, Web crawlers, robot exclusion, Web data mining, Metacrawler, Collaborative filtering, Web agents (web shopping, bargain finder,..), Economic, ethical, legal and political Issues.

Text Books/References:

1. Introduction to Information Retrieval. C.D. Manning, P. Raghavan, H. Schütze. Cambridge UP, 2008.
2. Modern Information Retrieval. R. Baeza-Yates, B. Ribeiro-Neto. Addison-Wesley, 1999.
3. Information Retrieval: Algorithms and Heuristics. D.A. Grossman, O. Frieder. Springer, 2004.
4. Managing Gigabytes. I.H. Witten, A. Moffat, T.C. Bell. Morgan Kaufmann, 1999.
5. The Geometry of Information Retrieval. C.J. van Risjbergen. Cambridge UP, 2004.

Course Outcomes (CO):

CO Number	Course Outcome
CO1	Ability to understand the nature of information and retrieval requirements.
CO2	Ability to use knowledge of data structures and indexing methods in information retrieval systems.
CO3	Ability to evaluate performance of retrieval systems.
CO4	Ability to choose clustering and searching techniques.
CO5	Ability to crawl information and explain different types of search algorithms.

CO-PO Mapping:

CO	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1	1	1	1	1	1
CO2	2	2	2	2	2	2
CO3	2	2	2	2	2	2
CO4	3	3	3	3	3	3
CO5	3	3	3	3	3	3
Total	11	11	11	11	11	11
Average	2.2	2.2	2.2	2.2	2.2	2.2
Eq. Avg. Attainment	2	2	2	2	2	2

8. Coding Theory	
L T P 4 , 0 , 0 : **4 Credits**	Prerequisites: *None*

Detailed Syllabus:

MODULE I

Shannon Theorem, Shannon capacity, Hamming's Theory, Error correcting codes, Linear codes, Impossibility results for codes, Mac Williams Identities, Linear programming bound.

MODULE II

The asymptotic perspective, Encoding, Decoding from erasures, Decoding RS codes, List decoding, linear time decoding, LDPC codes, Sipser-Spielman codes, Linear time encoding and decoding, Linear time and near optimal error decoding, Expander based constructions of efficiently, decodable codes, Some NP hard coding theoretic problems

MODULE III

Applications in complexity theory, Error correcting codes using Cryptography.

MODULE IV

Lossless Multicast Network Coding, Network coding in Lossy Networks, Security against adversarial errors, Error correction bounds for centralized network coding.

Text Books/References:

1. Tom Richardson, RudigerUrbanke, Modern Coding Theory, Cambridge University.
2. John b. Anderson and Seshadri Mohan, Source and Channel Coding: An Algorithm Approach, Springer.
3. G. Kabatiansky, E. Krouk and S. Semenov, Error Correcting Coding and Security for Data Networks, John Wiley & Sons Ltd.
4. Jiri Adamek, Foundations of Coding, Wiley Interscience Publication, John Wiley.
5. M. Medard and A. Sprintson, (editors): Network Coding – Fundamentals and Applications, Acadamic Press.
6. J. H. van Lint: Introduction to Coding Theory, Third Edition, Springer.

Course Outcomes (CO):

CO Number	Course Outcome
CO1	Understand Shannon's noisy coding theorem, Shannon capacity and entropy
CO2	Design of error correcting codes and decoding algorithms
CO3	Design and Analysis of light weight and code-based cryptosystems
CO4	Design of network coding algorithms for communication networks

CO-PO Mapping:

CO	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1	2	2	1		
CO2	1	1	2	2	2	1
CO3	2	1	3	3	2	1
CO4	1	1	2	3	2	1
Total	5	5	9	9	6	3
Eq. Avg. Attainment	1	1	2	2	2	1

9. Cyber Crime, Cyber Laws & IPR	
L T P 4 , 0 , 0 : **4 Credits**	Prerequisites: *None*

Detailed Syllabus:

MODULE I

Introduction to cyber crime and cyber law, cyber space and information technology, Nature and scope of cyber crime, Jurisdiction of cyber crime.

MODULE II

Important definitions under IT Act 2000, Cyber crime issues: unauthorized access, White collar crimes, viruses, malwares, worms, Trojans, logic bomb, Cyber stalking, voyeurism, obscenity in internet, Software piracy,

MODULE III

IT Act 2000, offences under IT Act and IT (amendment) Act, 2008. CRPC overview, Case studies, Role of intermediaries, Electronic evidence, Cyber terrorism, espionage, warfare and protected system.

MODULE IV

Overview of amended laws by the IT Act, 2000: The Indian Penal Code, 1860, The Indian EvidenceAct, 1872, The Banker's Book Evidence Act, 1891, The Reserve Bank of India Act, 1934, Cyber Theft and the Indian Telegraph Act, 1885. Relevant Case laws. Digital Signatures and certificate-legal issues.

MODULE V

Intellectual Property rights: Introduction to IP, Copyright, Related Rights, Trademarks, Geographical Indications, Industrial Design, Patents, Licensing and transfer of technology, WIPO Treaties, Copyrights Act, Patents Act, Trademarks Act.

Text Books/References:

1. Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives, RaghuSantanam, M. Sethumadhavan, Information Science Reference
2. Pfleeger, Charles P. and Shari L. Pfleeger. Security in Computing, 4th Edition. Upper SaddleRiver, NJ: Prentice Hall.
3. Cybercrime: Security and Surveillance in the Information Age, Douglas Thomas; BrianLoader
4. Computer Crime: A Crime-Fighters Handbook by David Icove
5. Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities, Peter N. Grabosky
6. Cyberlaw – The Indian Perspective By Pavan Duggal, Saakshar Law Publications.
7. Jonathan Rosenoer,"Cyber Law: The law of the Internet", Springer-Verlag, 1997
8. Mark F Grady, FransescoParisi, "The Law and Economics of Cyber Security", CambridgeUniversity Press,

Course Outcomes (CO):

CO Number	Course Outcome
CO1	To describe the cyber world and cyber law in general and about the various facets of cyber crimes
CO2	Explore the Legal and Policy Developments in Various Countries to Regulate Cyberspace
CO3	Give Learners in Depth Knowledge of Information Technology Act and Legal Frame Work of Right to Privacy, Data Security and Data Protection.
CO4	To clarify the Intellectual Property issues in the cyber space and the growth and development of the law in this regard

CO-PO Mapping:

CO	PO1	PO2	PO3	PO4	PO5	PO6
CO1		1	1	1	1	1
CO2		2	2		1	1
CO3	1	1	1	1		
CO4	1	1	2	1	1	2
Total	2	5	6	3	3	4
Eq. Avg. Attainment	1	1	2	1	1	1

10. Data Hiding	
L T P 4 , 0 , 0 : **4 Credits**	Prerequisites: *None*

Detailed Syllabus:

MODULE I

Introduction: data hiding models, security and privacy aspects, techniques for hiding data- Digital audio, video, images and text.

MODULE II

Stegnography: Introduction, how it is different from cryptography, Classification of stegnography algorithms: Transform-based, spatial domain, statistical, other, Applications of stegnography: Covert channels, audio data, military, e-commerce.

MODULE III

Watermarking: Introduction, how it is different from stegnography and cryptography, watermarking algorithms, watermarking applications, limitations in watermarking.

MODULE IV

Digital rights management issues: e-commerce, copyright protection, intellectual property Issues, digital signatures, authentication, case studies, business models.

MODULE V

Multimedia security and information assurance, visual cryptography, key management; Attacks and benchmarks for data hiding systems; Applications of data hiding technology in medicine, law enforcement, remote sensing, and e-commerce, Software for digital data hiding.

Text Books/References:

1. Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker, Digital Watermarking and Steganography, 2nd Edition, Morgan Kaufmann.
2. Michael T. Raggo and Chet Hosmer, Data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols, 1st Edition, Syngress.

Course Outcomes (CO):

CO Number	Course Outcome
CO1	Identify techniques for data hiding
CO2	Analyse models of watermarking
CO3	Identify different types of attacks
CO4	Apply data hiding techniques into different domains

CO-PO Mapping:

CO	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1	1	1	1		
CO2	2	2	2	2	1	1
CO3	1	1	1	1	1	1
CO4	1	1	2	2	2	1
Total	5	5	6	6	4	3
Eq. Avg. Attainment	1	1	2	2	1	1

11. Deep Learning	
L T P 4 , 0 , 0 : **4 Credits**	Prerequisites: *None*

Course Objectives:

1. To introduce the idea of Artificial Neural Networks and their applications.
2. To study and implement different architectures of Artificial Neural Networks.
3. To study and implement various optimization techniques on Artificial Neural Networks.
4. To enable design and deployment of deep learning models for machine learning problems.

Detailed syllabus:

MODULE I

Introduction: Artificial Intelligence and Deep Learning-a historical perspective, Artificial neural networks, Shallow neural networks, Deep neural networks, gradient descent, forward and backpropagation, computational graphs, linear and non-linear activation functions.

MODULE II

Optimization techniques: Regularization, Dropout, Batch Normalization, Vanishing/Exploding gradients, Mini-batch gradient, Gradient descent with momentum, RMSprop, Adam optimization, Learning rate decay, Local optima, Global optima. Hyperparameter tuning,

MODULE III

Convolutional Neural Networks: Basic operations: padding, stride, pooling; Classic convolutional models: LeNet-5, AlexNet, VGG, Modern Deep Convolutional models: ResNet, GoogleNet; Inception Network, 1-D convolutions, Object detection and Face Recognition with CNN.

MODULE IV

Recurrent Neural Networks: Sequence modelling, Types of Recurrent Neural Networks, Backpropagation through time, Language modelling and sequence generation, Word Embeddings, vanishing gradients with RNNs, Long-Short Term Memory (LSTM), Gated Recurrent MODULEs (GRU), Bidirectional LSTMs, Sequence-to-Sequence model, Attention Mechanism, Transformer Network.

MODULE V

Advanced topics: Deep Reinforcement Learning, Generative Adversarial Networks, Generative vs. Discriminative models, Deep Convolution GANS, Autoencoders.

References:

1. Charu C. Aggarwal, Neural Networks and Deep Learning- A textbook, 2018, Springer.
2. Ian Goodfellow, Yoshua Bengio, Aaron Courville, "Deep Learning (Adaptive Computation and Machine Learning series", MIT Press.
3. Nikhil Buduma, Nicholas Locascio, "Fundamentals of Deep Learning: Designing Next Generation Machine Intelligence Algorithms", O'Reilly Media.
4. Other online resources and research publications.

Course Outcomes (CO):

Course Outcome No.	Course Outcome
CO1	Students will be able to understand the mathematics and engineeringsciences behind functioning of artificial neural networks.
CO2	Students will be able to analyze the given dataset and data attributesfor designing a neural network-based solution.
CO3	Students will be able to identify different neural network architectures, neural network optimization techniques, and apply them on different problem domains.
CO4	Students will be able to design and deploy deep learning solutionsfor real-world applications with popular deep learning tools.

CO-PO Mapping:

CO	PO1	PO2	PO3	PO4	PO5	PO6
CO1	2	2	2	1	1	--
CO2	2	2	1	2	2	--
CO3	3	3	3	3	2	1
CO4	3	3	2	1	2	2
Total	10	10	8	8	8	3
Average Attainment	2.5	2.5	2	2	2	0.75
Eq. Average Attainment	3	3	2	2	2	1

12. Secure Coding	
L T P 4 , 0 , 0 : **4 Credits**	Prerequisites: *None*

Course Objectives:

This course aims to provide an understanding of the various security attacks and knowledge to recognize and remove common coding errors that lead to vulnerabilities. It gives an outline of the techniques for developing a secure application.

Detailed syllabus:

MODULE I:

Security, CIA Triad, Viruses, Trojans, and Worms In a Nutshell, Security Concepts- exploit, threat, vulnerability, risk, attack. Malware Terminology: Rootkits, Trapdoors, Botnets, Key loggers, Honeypots. Active and Passive Security Attacks. IP Spoofing, Tear drop,DoS, DDoS,XSS, SQL injection, Smurf, Man in middle, Format String attack. Types of Security Vulnerabilities- buffer overflows, Invalidated input, race conditions, access-control problems, weaknesses in authentication, authorization, or cryptographic practices. Access Control Problems.

MODULE II:

Need for secure systems: Proactive Security development process, Secure Software Development Cycle (S-SDLC), Security issues while writing SRS, Design phase security, Development Phase, Test Phase, Maintenance Phase, Writing Secure Code – Best Practices SD3 (Secure by design, default and deployment), Security principles and Secure Product Development Timeline.

MODULE III:

Threat modelling process and its benefits: Identifying the Threats by Using Attack Trees and rating threats using DREAD, Risk Mitigation Techniques and Security Best Practices. Security techniques, authentication, authorization. Defence in Depth and Principle of Least Privilege.

MODULE IV:

Secure Coding Techniques: Protection against DoS attacks, Application Failure Attacks, CPU Starvation Attacks, Insecure Coding Practices In Java Technology. ARP Spoofing and its countermeasures. Buffer Overrun- Stack overrun, Heap Overrun, Array Indexing Errors,FormatString Bugs. Security Issues in C Language: String Handling, Avoiding Integer Overflows and Underflows and Type Conversion Issues- Memory Management Issues, Code Injection Attacks, Canary based countermeasures using StackGuard and Propolice. Socket Security, Avoiding Server Hijacking, Securing RPC, ActiveX and DCOM.

MODULE V:

Database and Web-specific issues: SQL Injection Techniques and Remedies,Race conditions, Time of Check Versus Time of Use and its protection mechanisms. Validating Input and

Interprocess Communication, Securing Signal Handlers and File Operations. XSS scripting attack and its types – Persistent and Non persistent attack XSS Countermeasures and Bypassing the XSS Filters.

MODULE VI:

Testing Secure Applications: Security code overview, secure software installation. The Role of the Security Tester, Building the Security Test Plan. Testing HTTP-Based Applications, Testing File-Based Applications, Testing Clients with Rogue Servers.

References:

1. Writing Secure Code, Michael Howard and David LeBlanc,Microsoft Press.
2. Buffer Overflow Attacks: Detect, Exploit, Prevent by Jason Deckar,Syngress.
3. Threat Modeling, Frank Swiderski and Window Snyder,Microsoft Professional.

Course Outcomes (CO):

Course Outcome No.	Course Outcome
CO1	Understand the basics of secure programming.
CO2	Understand the most frequent programming errors leading to software vulnerabilities.
CO3	Identify and analyze security problems in software
CO4	Understand and protect against security threats and software vulnerabilities
CO5	Effectively apply their knowledge to the construction of secure software systems

CO-PO Mapping:

CO	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1	1				
CO2		2	1	1	2	1
CO3	1	3	2		2	2
CO4	1	1	2	1	2	1
CO5			2	1	2	2
Total	3	7	7	3	8	6
Eq. Average Attainment	1	1	1	1	2	1

13. Social Network Analysis	
L T P 4 , 0 , 0 : **4 Credits**	Prerequisites: *None*

Course Objectives:

To learn about structure and evolution of networks, to build a framework of network analysis that covers measures such as density, centrality, clustering, centralization, and specialization.

Detailed syllabus:

Module I

Networks- Concepts: nodes, edges, adjacency matrix, one and two-mode networks, node degree. Random network models: Erdos-Renyi and Barabasi-Albert- Concepts: connected components, giant component, average shortest path, diameter, breadth-first search, preferential attachment

Module II

Network centrality- Concepts: Betweenness, closeness, eigenvector centrality (+ PageRank), network centralization.

Module III

Community- Concepts: clustering, community structure, modularity, overlapping communities, Small world network models, optimization, strategic network formation and search-Concepts: small worlds, geographic networks, decentralized search Contagion, opinion formation, coordination and cooperation- Concepts: simple contagion, threshold models, opinion formation, unusual applications of SNA.

Module IV

SNA and online social networks- Concepts: how services such as Facebook, LinkedIn, Twitter, Couch Surfing, etc. are using SNA to understand their users and improve their functionality.

References:

1. John Scott, Social Network Analysis, 3rd Edition, SAGE,.
2. Wouter de Nooy, Andrej Mrvar, Vladimir Batagelj, Exploratory Social Network Analysis with Pajek, 2nd Revised Edition, Cambridge University Press,.
3. Patrick Doreian, Frans Stokman, Evolution of Social Networks, Routledge, 2013.
4. David Easley and Jon Kleinberg, Networks, Crowds, and Markets: Reasoning About a Highly Connected World, Cambridge University Press,.
5. Online Social Networks Security Principles, Algorithm, Applications, and Perspectives By Brij B. Gupta, Somya Ranjan Sahoo. ISBN 9780367619794 Published by CRC Press.

Course Outcomes (CO):

Course Outcome No.	Course Outcome
CO1	Understand various concepts in networks, dynamics and development of social structures
CO2	Analyze framework of network analysis and compare various random network models
CO3	Apply network centrality using various concepts like betweenness, closeness, page ranks etc.
CO4	Know about various community concepts like: clustering, community structure, modularity.
CO5	Understand how various social media networks are working and using SNA in their infrastructure.

CO-PO Mapping:

CO	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1	2	1	1		
CO2	1	2	1	2	1	2
CO3	1	3	3	3	2	2
CO4	1	1	1			
CO5	1	1	1	1	1	
Total	5	9	7	7	4	4
Attainment	1	2	1	1	1	1

14. Cyber Forensics, Audit & Investigation	
L T P 4 , 0 , 0 : **4 Credits**	Prerequisites: *None*

Detailed syllabus:

MODULE I

File system: CHS, LBA, HPA, write blockers, Extracting & recovering partitions, MBR, DOS partition table, Extended partition table, RAID; FAT file system: Architecture, File creation, File deletion; NTFS file system: Architecture, File creation, File deletion, Compression, encryption and indexing;

MODULE II

Extended file systems: EXT2, EXT3 and EXT4, Architecture, File creation, File deletion and Journaling; Apple File System (APFS); Other Disk structures; Windows and Linux boot process; Filesystem acquisition and recovery

MODULE III

Windows Forensic Analysis: Window artifacts, Evidence volatility, System time, Logged on user(s), Open files, MRUs, Network information, Process information, Service information, Windows Registry, Start up tasks, Memory dumping; Document Forensics: PDF structure, PDF analysis, MSOffice Document structure and analysis, Macros, Windows thumbnails, Android Thumbnails

MODULE IV

Mobile Forensics: SIM Card, Android architecture, Android File System, Android application, Android SDK,Android Debug Bridge, Memory & SIM acquisition; Virtual Machines, Network Forensics; Cyber crime investigation: Pre investigation, SOP for Investigation; Case scenarios: social media crime, Online defacement crime, Email investigation; CDR Analysis

MODULE V

Auditing: Internal Audit and IT Audit Function, IT Governance, Frameworks, Standards, and Regulations, Identifying information assets, Risk assessment, Risk management, Types of Auditing, ISO 27001, PCIDSS

References:

1. Computer Evidence - Collection and Preservation.Brown, C.L.T. Course Technology Cengage Learning.
2. Guide to Computer Forensics And Investigations Nelson, Bill ; Phillips, Amelia; Enfinger, Frank; Steuat, Christopher Thomson Course Technology.
3. Computer Forensics – Computer Crime Scene Investigation.Vacca, John R. Charles RiverMedia

4. Bunting, Steve and William Wei. EnCase Computer Forensics: The Official EnCE: EnCaseCertifed Examiner Study Guide. Sybex,
5. Incident Response: Computer Forensics, Prosise, Chris, Kevin Mandia, and Matt Pepe, McGraw-Hill, 2014
6. IT Security Risk Control Management: An Audit Preparation Plan, Raymond Pompon, Apress 2016
7. Carrier, Brian. File System Forensic Analysis. Addison-Wesley Professional

Course Outcomes (CO):

Course Outcome No.	Course Outcome
CO1	Learn about the importance of digital forensic principles and procedures, legal considerations, digital evidence controls.
CO2	Obtain and analyze digital information for possible use as evidence in civil, criminal or administrative cases.
CO3	Illustrate forensic duplication and file system analysis.
CO4	Make a solid foundational grounding in computer networks, operating systems, file systems, hardware, and mobile devices to digital investigations and to the protection of computer network resources from unauthorized activity

CO-PO Mapping:

CO	PO1	PO2	PO3	PO4	PO5	PO6
CO1	2	2	2	1		
CO2	2	2	1	1	2	1
CO3		3	1	1		1
CO4		1	2	1	1	
Total	4	8	6	4	3	2
Eq. Average Attainment	1	2	2	1	1	1

15. Cloud & IoT Security	
L T P 4 , 0 , 0 : **4 Credits**	Prerequisites: *None*

Course Objectives:

1. To understand the fundamentals of Internet of Things (IoT) and Cloud Computing.
2. Explore the cryptographic fundamentals for IoT.
3. Ability to understand the Security requirements in IoT.
4. To apply the concept of Internet of Things in the real world scenario.

Detailed syllabus:

MODULE I

Fundamentals of IoT and Cloud Computing: Evolution of Internet of Things, Enabling Technologies, IoT Architectures: oneM2M, IoT World Forum (IoTWF) and Alternative IoT models, Simplified IoT Architecture and Core IoT Functional Stack, Fog, Edge and Cloud in IoT, Functional blocks of an IoT ecosystem, Sensors, Actuators, Smart Objects and Connecting Smart Objects.

MODULE II

IoT Architectures and Protocols: M2M high-level ETSI architecture, IETF architecture for IoT, OGC architecture. IoT reference model: Domain model, information model, functional model, communication model. IoT reference architecture. Protocol Standardization for IoT: Efforts, M2M and WSN Protocols, SCADA and RFID Protocols. IoT Access Technologies: Physical and MAC layers, topology and Security of IEEE 802.15.4, LoRaWAN, Network Layer: IP versions, Constrained Nodes and Constrained Networks. Optimizing IP for IoT: From 6LoWPAN to 6Lo, Routing over Low Power and Lossy Networks, Application Layer Protocols: CoAP and MQTT.

MODULE III

Securing the IoT: Security Requirements in IoT Architecture, Security in Enabling Technologies, Security Concerns in IoT Applications. Security Architecture in the Internet of Things, Security Requirements in IoT, Insufficient Authentication/Authorization, Insecure Access Control, Threats to Access Control, Privacy, and Availability, Attacks Specific to IoT. Vulnerabilities. Secrecy and Secret-Key Capacity, Authentication/Authorization for Smart Devices, Transport Encryption, Attack & Fault trees.

MODULE IV

Cloud Security for IoT: Cloud services and IoT: offerings related to IoT from cloud service providers, Cloud IoT security controls, and an enterprise IoT cloud security architecture. New directions in cloud enabled IoT computing.

MODULE V

Applications & Case Study: Real world design constraints, Applications, Asset management, Industrial automation, smart grid, Commercial building automation, Smart cities, participatory sensing. Data Analytics for IoT. Software & Management Tools for IoT Cloud Storage Models & Communication APIs. Cloud for IoT: Amazon Web Services for IoT.

References:

1. Xu, L. D., & Li, S. (2017). Securing the Internet of Things. Elsevier.
2. Weippl, E. (2018). Internet of Things Security: Fundamentals, Techniques and Applications. River Publishers.
3. Russell, B., & Van Duren, D. (2016). Practical internet of things security. Packt Publishing Ltd.
4. Hu, F. (2016). Security and privacy in Internet of things (IoTs): Models, Algorithms, and Implementations. CRC Press.
5. Zhou, H. (2012). The internet of things in the cloud: a middleware perspective. CRC press.
6. Hersent, O., Boswarthick, D., & Elloumi, O. (2011). The internet of things: Key applications and protocols. John Wiley & Sons.
7. Gupta, B., Agrawal, D., Handbook of Research on Cloud Computing and Big Data Applications in IoT, IGI Global, USA, ISBN13: 9781522584070, 2019.
8. Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the internet of things: a survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 17(3), 1294-1312.

Course Outcomes (CO):

Course Outcome No.	Course Outcome
CO1	Identify different issues in cloud and IoT security.
CO2	To analyze protocols and reference architectures developed for cloud and IoT.
CO3	To identify and understand various applications of cloud and IoT.

CO-PO Mapping:

CO	PO1	PO2	PO3	PO4	PO5	PO6
CO1	2	1	2			--
CO2	2	3	2	1		--
CO3	2	3	2	1		1
Total	6	7	6	2		1
Eq. Average Attainment	2	2	2	1		

16. Big Data Analytics	
L T P 4 , 0 , 0 : **4 Credits**	Prerequisites: *None*

Course Objectives:

1. To explore the fundamental concepts of big data analytics using intelligent techniques.
2. To learn to use various techniques for mining data stream.
3. To understand the applications using Map Reduce Concepts.
4. To understand the programming tools and frameworks in Hadoop distributed system.
5. To acquire the knowledge of different big data issues.

Detailed syllabus:

MODULE I
Introduction to big data: Introduction to Big Data Platform; Challenges of Conventional Systems, Intelligent data analysis; Nature of Data, Analytic Processes and Tools, Analysis vs Reporting, the four dimensions of Big Data: volume, velocity, variety, veracity, Drivers for Big Data, Introducing the Storage, Query Stack, Revisit useful technologies and concepts, Real-time Big Data Analytics.

MODULE II
Mining data streams: Introduction to Streams Concepts; Stream Data Model and Architecture, Stream Computing, Sampling Data in a Stream; Filtering Streams; Counting Distinct Elements in a Stream; Estimating Moments; Counting Oneness in a Window; Decaying Window, Real time Analytics Platform (RTAP) Applications, Case Studies, Real Time Sentiment Analysis, Stock Market Predictions.

MODULE III
Distributed File Systems: Hadoop Distributed File System History of Hadoop- the Hadoop Distributed File System; Components of Hadoop Analyzing the Data with Hadoop- Scaling Out- Hadoop Streaming- Design of HDFS-Java interfaces to HDFS Basics- Developing a Map Reduce Application-How Map Reduce Works-Anatomy of a Map Reduce Job Run-Failures-Job Scheduling-Shuffle and Sort; Task execution, Map Reduce Types and Formats- Map Reduce Features Hadoop environment. Data Consistency.

MODULE IV
Overview of Spark Ecosystem, Understanding Spark Cluster Modes on YARN, RDDs (Resilient Distributed Datasets), General RDD Operations: Transformations & Actions, Common Spark Use Cases, Data Frames and Spark SQL, Analyzing Data with Pig, NoSQL and HBase

MODULE V
Scalable Algorithms: Mining large graphs, with focus on social networks and web graphs. Centrality, similarity, a 11-distances sketches, community detection, link analysis, spectral techniques. Map-reduce, Pig Latin, and NoSQL using MongoDB, Algorithms for detecting similar items, Recommendation systems, Data stream analysis algorithms, clustering algorithms, Detecting frequent items.

MODULE VI

Frameworks and Big Data Issues: Applications on Big Data Using Pig and Hive; Data processing operators in Pig; Hive services; HiveQL; Querying Data in Hive, fundamentals of HBase and ZooKeeper, IBM InfoSphere BigInsights and Streams. Privacy, Visualization, Compliance and Security, Structured vs Unstructured Data.

Text Books:

1. Ohlhorst, Frank J. Big data analytics: turning big data into big money. Vol. 65. John Wiley & Sons, 2012.
2. Russom, Philip. "Big data analytics." TDWI best practices report, fourth quarter 19, no. 4 (2011): 1-34.
3. Marr, Bernard. Big Data: Using SMART big data, analytics and metrics to make better decisions and improve performance. John Wiley & Sons, 2015.
4. LaValle, Steve, Eric Lesser, Rebecca Shockley, Michael S. Hopkins, and Nina Kruschwitz. "Big data, analytics and the path from insights to value." MIT sloan management review 52, no. 2 (2011): 21-32.
5. Leskovec, Jure, Anand Rajaraman, and Jeffrey David Ullman. Mining of massive data sets. Cambridge university press, 2020.
6. Tom White "Hadoop: The Definitive Guide" Third Edition, O'reilly Media, 2012.
7. Arshdeep Bahga, Vijay Madisetti, "Big Data Science & Analytics: A Hands On Approach ",VPT, 2016

Course Outcome (CO):

CO No.	Course Outcome
CO1	Acquire the fundamental concepts of big data analytics using Intelligent techniques.
CO2	To learn how to use various techniques for mining data stream.
CO3	Map Reduce Concepts implementation in Big data problem.
CO4	Acquire the knowledge of programming tools and frameworks in Hadoop distributed system.
CO5	To explore different issues in big data domain.

CO-PO Mapping:

Course Outcome	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	1	1	1	1	1	1
CO-2	1	2	2	1	1	1
CO-3	2	2	2	1	1	1
CO-4	3	2	2	1	2	2
CO-5	3	3	2	2	2	2
Total	10	10	9	6	7	7
Average	2	2	1.8	1.2	1.4	1.4
Attainment	2	2	2	1	1	1

17. Ethical Hacking	
L T P 4 , 0 , 0 : **4 Credits**	Prerequisites: *None*

Course Objectives:

1. The aim of the course is to introduce the methodologies and framework of ethical hacking for enhancing the security.
2. The course includes-Impacts of Hacking; Types of Hackers; Information Security Models; Information Security Program; Business Perspective; Planning a Controlled Attack; Framework of Steps (Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Deliverable and Integration)

Detailed syllabus:

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

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

MODULE – III : Preparing for a Hack:
Technical Preparation, Managing the Engagement Reconnaissance: Social Engineering, Physical Security, Internet Reconnaissance

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

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

Text Books/References:

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

Course Outcome (CO):

CO No.	Course Outcome
CO1	Gain the knowledge of the use and availability of tools to support an ethical hack
CO2	Gain the knowledge of interpreting the results of a controlled attack
CO3	Understand the role of politics, inherent and imposed limitations and metrics fo planning of a test
CO4	Comprehend the dangers associated with penetration testing

CO-PO Mapping:

Course Outcome	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	1	1	1	1	1	
CO-2	1	2	2	1	1	
CO-3	2	2	2	1	1	
CO-4	1	1	1	1	2	
Total	5	6	6	4	5	
Attainment	1	2	2	1	1	

18. Wireless Network Security	
L T P 4 , 0 , 0 : **4 Credits**	Prerequisites: *None*

Detailed syllabus:

MODULE I
Wireless Networking Trends, Key Wireless Physical Layer Concepts: Frequency, Wavelength, Phase, Coding and modulation, Shannon Theorem, Hamming Distance, Multiple Access Methods, Doppler Shift; Signal Propagation: Reflection, Diffraction, Scattering, Fading, Shadowing, Multipath, MultiAntenna Systems, Beam forming, MIMO, OFDM; Wireless Local Area Networks: IEEE802.11, Amendments; Wireless Personal Area Networks.

MODULE II
GSM: Overview, Architecture, GSM Security Principles; General Packet Radio Services (GPRS): Overview, Architecture; Universal Mobile Telecommunication System (UMTS): Overview, Architecture and Subsystems; LTE: Overview, Architecture and Subsystems;

MODULE III
Radio Frequency Identification (RFID); WiMAX (Physical layer, Media access control, MobilityandNetworking); Multi hop wireless networks: Position & topology base ad-hoc routing protocols, Proactive and Reactive routing protocols. Route disruption, diversion, routing state based attacks, SRP, Ariadne, SAODV, ARAN, SMT secure routing protocols, Wireless Sensor Networks,

MODULE IV
Security of wireless networks: GSM, UMTS, WEP, IEEE 802.11i, Public Wifi hotspots, Bluetooth;
Vehicular Ad-hoc Networks: vulnerabilities, challenges, Security architecture

MODULE V
Naming & addressing principles, attacks and protection techniques, Misbehavior at MAClayer of CSMA/CA, its impact and preventive measures, Mobile IPv4, Mobile IPv6, TCP over Wireless Networks.

Text Books/References:

1. Jochen Schiller, "Mobile Communications", PHI.
2. K Makki, P Reiher,et. all. "Mobile and Wireless Network Security and Privacy",Springer.
3. LeventeButtyan, J P Hubaux. "Security and Cooperation in Wireless Networks", CambridgeUniversity Press.
4. Frank Adelstein, Sandeep KS Gupta, Golden Richard, Fundamentals of Mobile and Pervasive Computing, McGraw-Hill
5. Butty L. &Hubaux J.P.: Security and Cooperation in Wireless Networks: ThwartingMalicious and Selfish Behavior in the Age of Ubiquitous Computing, Cambridge University Press.

6. Wireless Ad hoc and Sensor Networks – Protocols, Performance and Control, Jagannathan Sarangapani, CRC Press, Taylor & Francis Group,

Course Outcome (CO):

CO No.	Course Outcome
CO1	To understand the architecture of wireless network and associated technologies.
CO2	Familiarize with the issues and technologies involved in designing a wireless and mobile system that is robust against various attacks.
CO3	Gain knowledge and understanding of the various ways in which wireless networks can be attacked and tradeoffs in protecting networks.
CO4	Identify security threats in wireless networks and design strategies to manage network security

CO-PO Mapping:

Course Outcome	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	1	1	1	1	1	1
CO-2	1	2	2		2	1
CO-3	2	2	2	1	2	1
CO-4	1	2	2	1	2	1
Total	5	7	7	3	7	4
Attainment	1	2	2	1	2	1