M. Tech.

Computer Science and Engineering

(CSE)

Curriculum and Syllabus

Department of Computer Science and Engineering

M.Tech. Computer Science and Engineering

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 Computer Science (Core – 1)	CSCS101	3-1-0	100	25	0	4	70
2	Design and Analysis of Algorithms (Core – 2)	CSCS103	3-0-2	100	0	50	4	85
3	Machine Learning (Core – 3)	CSCS105	3-0-2	100	0	50	4	85
4	Core Elective -1	CSCS1XX	3-1-0 / 3-0-2	100	0 / 25	0 / 50	4	70 / 85
5	Core Elective - 2	CSCS1XX	3-0-2	100	0	50	4	85
						Total	**20**	**395 - 410**
6	Vocational Training / Professional Experience (Optional) (Mandatory for Exit)	CSCSV91 CSCSP93	0-0-10				5	200 (20 x 10)
	Second Semester							
1	Wireless Network and Mobile Computing (Core – 4)	CSCS102	3-0-2	100	0	50	4	85
2	Distributed System (Core – 5)	CSCS104	3-0-2	100	0	50	4	85
3	Elective - 3	CSCS1XX	3-1-0 / 3-0-2	100	0 / 25	0 / 50	4	70 / 85
4	Elective - 4	CSCS1XX	3-0-2	100	0	50	4	85
5	Institute Elective*	CSCS1XX	3-0-0 / 3-0-2 / 3-1-0	100	0 / 25	0 / 50	3 / 4	55 / 70 / 85
6	Mini Project	CSCS106	0-0-4	-	-	100	2	70
						Total	**21 – 22**	**450 - 495**
7	Vocational Training / Professional Experience (Optional) (Mandatory for Exit)	CSCSV92 CSCSP94	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	CSCS295	-	-	-	$350^{\$}$	14	560
						Total	**20 - 22**	**700 - 720**
	Fourth Semester							
1	Dissertation	CSCS296	-	-	-	$600^{\$}$	20	800
						Total	**20**	**800**

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, ɸ 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	
CSCS111	Computer Vision and Image Processing	3-0-2
CSCS113	Advanced Database Management System	3-0-2
CSCS115	High Performance Computing	3-0-2
CSCS117	Foundation of Data Science	3-0-2
CSCS119	Embedded Systems Design	3-0-2
CSCS121	Speech and Audio Processing	3-0-2
CSCS123	Cloud Computing and Big Data Analytics	3-0-2
CSCS125	Principles of Information Security and Privacy	3-0-2
CSCS127	Research Methodology in CSE	3-1-0
CSCS129	Probabilistic Graphical Models	3-1-0
CSCS131	Artificial Intelligence	3-0-2
CSCS133	Cyber Physical Systems	3-0-2
CSCS135	Digital Forensics	3-0-2
CSCS139	Identity and Access Management	3-0-2
CSCS141	Software Security	3-0-2
CSCS143	Security and Privacy in Resource Constrained Environments	3-0-2
CSCS145	Blockchain Fundamentals and Use cases	3-0-2
CSCS147	Network Security	3-0-2
CSCS149	Modern Cryptography	3-1-0
CSCS151	Information Retrieval	3-0-2
CSCS153	Big data analytics and large-scale computing	3-0-2
	Core Elective 3 and 4	
CSCS112	ANN and Deep Learning	3-0-2
CSCS114	Introduction to Formal Specification and Verification	3-0-2
CSCS116	Natural Language Processing	3-0-2
CSCS118	Reinforcement Learning	3-0-2
CSCS120	Data Mining and Data Warehousing	3-0-2
CSCS122	Data Science for Software Engineering	3-0-2
CSCS124	Security and Privacy in Social Networks	3-0-2
CSCS126	Foundations of Privacy Engineering	3-1-0
CSCS128	Malware Analysis and Mitigation	3-0-2
CSCS130	Secure Software Engineering	3-0-2
CSCS132	Mobile Security and Penetration Testing	3-0-2
CSCS134	Bitcoin and Cryptocurrency Technologies	3-0-2
CSCS136	Security Protocols	3-0-2

CSCS138	Hardware Security	3-0-2
CSCS140	Machine Learning for Security	3-0-2
	Institute Elective	
CSCS172	Social Networks	3-0-0
CSCS174	Cyber Laws	3-0-0
CSCS176	Ethical Hacking and Penetration Testing	3-0-2

M. Tech. I CSE Semester – I	**L**	**T**	**P**	**C**
CSCS101: MATHEMATICAL FOUNDATIONS OF COMPUTER SCIENCE (CORE-1)	**3**	**1**	**0**	**4**

Course Objective	
1	To learn the fundamental concepts of set theory, functions, probability.
2	To study the graph theory, its applications and combinatorics problem solving arising in many applications.
3	To learn different statistical inference procedures, probability distributions and random processes.
4	To enable the student for applying the knowledge of linear algebra and statistical analysis in different field of computer science and engineering.
5	To design an efficient solution using linear algebra and statistical methods for real time problems.

INTRODUCTION	**(04 Hours)**
Set theory, Logic and Proofs, Conditional Propositions, Logical Equivalence, Predicates, Quantifiers, Combinatorics	
FUNCTIONS AND RELATIONS	**(04 Hours)**
Types of functions, Recursive functions, Computable and non-computable functions, Representations of relations, Composition and properties of relations	
GRAPH AND AUTOMATA	**(09 Hours)**
Different types of graphs, Trees, Basic Concepts Isomorphism and Sub graphs, Multi graphs and Euler circuits, Hamiltonian graphs, Chromatic Numbers, Graph and Tree processing algorithms, Different types of Automata, Formal Languages, Regular expressions, Context free grammars	
PROBABILITY AND RANDOM VARIABLES	**(09 Hours)**
Overview of Sample points and Sample spaces, Events, Bayes theorem, Probability axioms, Joint and conditional probability, Random variables, Discrete and continuous random variables, Random vectors, Transformation of continuous random variables and vectors by deterministic functions, Density functions of transformed continuous random variables and vectors, Multivariate random variables, Moments and moment generating functions, Functions of random variables.	
RANDOM PROCESSES	**(09 Hours)**
Random variable vs. Random process, Bernoulli random process, Binomial process, Statistical averages, Ensemble and time averages, Weak and strict sense stationarity of a random process, Ergodicity, Autocorrelation and Auto covariance functions of random processes and its relation to spectra, Poisson process, Gaussian process, Martingale model and Markov Chains.	
ESTIMATION AND STATISTICAL ANALYSIS	**(10 Hours)**
Estimation of parameters from data, Maximum likelihood estimation, Maximum a posterior estimation, Consistency and Efficiency of Estimators, Stochastic State Estimation and MSE of an Estimator, Estimation of Gaussian Random Vectors, Linear minimum mean square error estimation, Hypothesis testing, Significance level, Types of errors: Type-I and Type-II, Significance Test, Chi-Squared, Student-t test, Normality test, Cramer-Rao bound on estimators, Chebyshev inequality, KullbackLeibler divergence, Applications.	
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. Kenneth H. Rosen, “Discrete Mathematics and Its Applications”, McGraw-Hill, 8th Edition, 2021.
2. Gersting J.L., “Mathematical Structure for Computer Science”, W.H. Freeman and Co., 3rd Edition, 1993.
3. A. Papoulis and S. U. Pillai, “Probability, Random Variables and Stochastic Processes”, 4th Edition, 2017.
4. W B Davenport, “Probability and Random Processes - an introduction for application scientists and engineers”, McGraw Hill, 1970.
5. S. M. Ross, Introduction to Probability Models”, Academic Press, 12th Edition, 2019.

Course Outcomes **At the end of the course, students will**	
CO1	have a knowledge of the basic concepts and problems of set theory, predicates and logic
CO2	be able to use functions, graphs, trees, automata and formal languages for problem solving
CO3	be able to analyze/interpret quantitative data verbally, graphically, symbolically and numerically.
CO4	be able to evaluate and compare the results using different linear algebraic and statistical techniques.
CO5	be able to use linear algebra for optimization and integrate statistical models for solving real life applications.

M. Tech. I (CSE) Semester – I	**L**	**T**	**P**	**C**
CSCS103: DESIGN AND ANALYSIS OF ALGORITHMS (CORE-2)	**3**	**0**	**2**	**4**

Course Objective	
1	To understand paradigms and approaches used to analyze and design algorithms and to appreciate the impact of algorithm design in practice.
2	To analyze 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 analyze 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 Case 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, Motivation.	
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.	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

List of Practical (Problem Statements will be changed every year and will be notified on Website.)	
1.	Designing algorithms for trivial computational problems and doing their empirical timing analysis.
2.	Designing algorithms using divide and conquer technique and doing their empirical timing analysis.
3.	Designing algorithms using greedy technique and doing their empirical timing analysis.
4.	Designing algorithms using dynamic programming and doing their empirical timing analysis.
5.	Backtracking & branch bound approach to design algorithms.
6.	Designing Approximation algorithms to solve the hard computational problems.

BOOKS RECOMMENDED

1. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein, "Introduction to Algorithms", The MIT Press.
2. Donald E. Knuth, "The Art of Computer Programming, Vol. 1, Vol. 2 and Vol. 3", Narosa/Addison Wesley, New Delhi/London.
3. Sara Baase, Allen V. Gelder, "Computer Algorithms", Pearson Education.
4. Ellis Horowitz, SartajSahni, "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. 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) Semester – I	L	T	P	C
CSCS105: MACHINE LEARNING (CORE-3)	**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 apply different concepts for the machine learning problems
3	To apply and analyze different supervised and unsupervised learning approaches as per the suitability of the problem
4	To understand and evaluate machine learning methods to use them
5	To design solution of problem using different machine learning approaches

INTRODUCTION	**(04 Hours)**
Pattern Representation, Concept of Pattern Recognition, Basics of Probability, Bayes’ Decision Theory, Maximum-Likelihood and Bayesian Parameter Estimation, Error Probabilities, Learning of Patterns, Modeling, Regression, Discriminant Functions, Linear Discriminant Functions, Decision surface, Learning Theory, Fisher Discriminant Analysis.	
LINEAR ALGEBRA FOR ML	**(06 Hours)**
SUPERVISED LEARNING ALGORITHMS	**(07 Hours)**
Gradient Descent, Linear Regression, Support Vector Machines, K-Nearest Neighbor, Naïve Bayes, Bayesian Networks, Classification, Decision Trees, ML and MAP Estimates, Overfitting, Regularization, Bayes Classification, Nearest Neighbor Classification, Cross Validation and Attribute Selection, Bayesian Decision Theory, Losses and Risks, Bayesian Networks, Parametric Methods: Gaussian Parameter Estimation, Maximum Likelihood Estimation, Bias and Variance, Bayes' Estimator, Bayesian Estimation, Parametric Classification, Regression, Naive Bayes, Hidden Markov Models, Support Vector Machines, Decision Trees.	
NEURAL NETWORKS AND LEARNING ALGORITHMS	**(06 Hours)**
Artificial Neural Networks, Perceptron, Multilayer Networks, Back Propagation, Deep Neural Networks, Convolutional Neural Networks, Recurrent Neural Networks; Linear Discrimination, Multilayer Perceptrons: Multilayer Perceptrons, Backpropagation Algorithm, Nonlinear Regression, Convergence, Overtraining, Dimensionality Reduction, Gradient Descent, Recurrent Networks, Cross-Validation and Resampling Methods, Bootstrapping.	
UNSUPERVISED LEARNING ALGORITHMS	**(06 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, Nonparametric techniques for density estimation, Parzen-window method.	
MISCELLANEOUS TOPICS	**(06 Hours)**
Dimensionality Measuring Error, Interval Estimation, Hypothesis Testing, Reduction, Feature Selection, Principal Component Analysis, Pattern Analysis using Eigen Decomposition, Principal Component Analysis, Parzen-windows Method, Model Selection and Theory of Generalization, In-sample and Out-of-sample Error, Vapnik-Chervonenkis (VC) Dimension, VC Inequality, VC Analysis.	
APPLICATIONS	**(10 Hours)**
Signal Processing, Image Processing, Biometric Recognition, Face and Speech Recognition, Information	

Retrieval, Natural Language Processing.	
Practical and mini-projects will be based on the coverage of the above topics.	**(30 Hours)**
	(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)

List of Practical (Problem Statements will be changed every year and will be notified on Website.)	
1.	Implement classification and regression techniques
2.	Implement clustering and statistical modeling methods
3.	Implement various dimensionality reduction techniques
4.	Implement neural networks and non-parametric techniques
5.	Implement mini-project based on machine learning approaches

BOOKS RECOMMENDED

1. Richard O. Duda, Peter E. Hart, David G. Stork, “Pattern Classification”, 2nd Edition, 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 Taylor and NelloCristianini, “Kernel methods for pattern analysis” Cambridge 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 Edition, Academic Press, 2009.

Course Outcomes **At the end of 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-II(CSE) Semester – II	**L**	**T**	**P**	**C**
CSCS102: WIRELESS NETWORK AND MOBILE COMPUTING (CORE-4)	**3**	**0**	**2**	**4**

Course Objective	
1	To learn fundamental concepts in the area of mobile computing and overview of wireless communication networks area and its applications.
2	To understand various terminology, principles, devices, protocols, algorithms and different methodologies used in wireless communication networks.
3	To learn various wireless channel access schemes like multiple division techniques, modulations scheme, topology of mobile communication systems, cellular and adhoc network
4	To learn various issues and challenges of computing in wireless network, and different computing models and algorithms for ubiquitous computing.
5	To develop the design skills for protocols and mobile applications for different applications which are robust and efficient for operating in wireless environment.

INTRODUCTION	**(06 Hours)**
Wired Network vs. Wireless Network, Overview of Wireless Applications, Wireless Transmission: Path loss, Multi-path propagation, Doppler shift, Fading, Time Division Multiplexing, Frequency Division Multiplexing, Spread Spectrum Technique, Direct sequence spread spectrum, Frequency hopping spread spectrum, CDMA - code division multiple access, OFDM - Orthogonal Frequency Division Multiple Access, Satellite Communication, Statistical Modeling of multipath fading channel, Frequency selective and non-selective fading channels, Flat fading channels, Path-loss, Propagation Model, Shadowing, Rayleigh Fading, Equalization, Channel Modeling and Estimation, Blind Channel Estimation, AWGN Channel.	
CELLULAR SYSTEM	**(12 Hours)**
Cellular Network Organization, Cellular System Evolution, Cellular Fundamentals: Capacity, Topology, Operation of Cellular Systems, Cellular geometry, Frequency reuse, Cell spitting, Sectoring, Handoff, Power control, Case study: Global System for Mobile communication (GSM) Network, General Packet Radio Service (GPRS), Code Division Multiple Access (CDMA 2000), Cordless System, Wireless Local Loop, Mobility Management-Location Management, HLR-VLR scheme, Hierarchical scheme, Predictive location management schemes, Types of interference, Estimation of adjacent channel interference and co channel interference, Trunk efficiency, Grade of service, Blocking probabilities, Propagation models, Frequency management and channel assignment. Packet delivery and handover management, Location management, Tunnelling and encapsulation, Route optimization.	
AD HOC WIRELESS NETWORK	**(09 Hours)**
Cellular vs. Ad Hoc, Applications, Issues, MAC protocols, Routing Protocols, Transport Layer Protocol, Multicasting protocols, Security protocols, Key management, Issues and Challenges in Security provisioning, Security attacks, Secured routing, Standards: IEEE 802.11, Wi-Fi, Wireless Broadband-Wi-MAX, Bluetooth, IEEE 802.15, Security in Wireless Network, Hyper LAN.	
MULTI INPUT MULTI OUTPUT	**(09 Hours)**
Single user modulation techniques, Multiple access techniques, Matched filter, RAKE receiver, Equalization, Multi user detection, Blind multi user detection, Bayesian multiuser detection in Gaussian noise, Multi input and Multi Output Communication, MIMO Channel Estimation, MIMO Channel Capacity, Transmitter Diversity, Receiver Diversity.	
MOBILE COMPUTING	**(09 Hours)**

Mobile Computing, Issues: Resource Management, Interference, Bandwidth, Frequency reuse, Mobile Data Transaction Models, Data handling in Mobile computing, Client server computing, Data recovery and query processing, Mobile operating system, Mobile Ad-hoc and sensor network, Personal area network, Data synchronization, Service management, Mobile File system File Systems, Mobility Management, Wireless Application Protocol, Security issues in Mobile.	
Practical and mini-projects will be based on the coverage of the above topics.	**(30 Hours)**
	(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)

List of Practical (Problem Statements will be changed every year and will be notified on Website)	
1	To understand and learn the basic application development using Android platform and to demonstrate the communication between two different android devices.
2	To set up and analyse the wireless networks system considering multiple nodes and different parameters using network simulation tools.
3	To implement File Transfer, Access and Authentication based applications for mobile computing
4	To compare ad-hoc routing protocols using simulation tools like NS3, Tiny OS, OPNET and OMNET++
5	To work on mini project based on tracking, localization and routing in wireless network.

BOOKS RECOMMENDED

1. William Stallings, "Wireless Communications & Networks", 2nd Ed., Pearson Education India, Reprint 2007.
2. Jochen Schiller, "Mobile Communications", 2nd Ed., Pearson Education India, reprint 2007.
3. T S Rappaport, "Wireless Communications: Principles & Practice", 2nd Ed., Pearson Education, 2002.
4. Raj Kamal, “Mobile Computing”, Oxford University Press, 2007.
5. C. Siva Ram Murthy and B. S. Manoj, “Ad Hoc Wireless Networks: Architectures and Protocols”, Pearson education 2007.

ADDITIONAL BOOKS RECOMMENDED

1. Sandeep Singhal, "The Wireless Application Protocol", Addison Wesley, India, reprint 2001.
2. C E Perkins, "Ad Hoc Networking", Addison Wesley, 2000.
3. Asoke K Talukder, Roopa R Yavagal, “Mobile Computing: Technology, Applications and Service Creation”, Tata McGraw-Hill, Third reprint 2006.
4. Xiaodong Wang, H. Vincent Poor, “Wireless Communication Systems: Advanced Techniques for Signal Reception”, Pearson Education, 2006.
5. Gottapu Sasibhushana Rao, “Mobile Cellular Communication”, Pearson, 2013.

Course Outcomes **At the end of the course, students will**	
CO1	have knowledge of fundamentals of wireless communications and mobile computing.
CO2	be able to apply the knowledge of TCP/IP for designing the systems for mobile and wireless networks.
CO3	be able to analyze security, energy efficiency, mobility, scalability and their unique characteristics in wireless networks.
CO4	be able to evaluate different protocols and mobile application developed for the cellular and ad-hoc wireless networks.
CO5	be able to design and innovate a solution for the issues and problems related to wireless networks and mobile computing.

M. Tech. I (CSE) Semester – II	**L**	**T**	**P**	**C**
CSCS104: DISTRIBUTED SYSTEMS **(CORE -5)**	**3**	**0**	**2**	**4**

Course Objective	
1	To learn the principles, architectures, algorithms and programming models used in distributed systems
2	To understand design and implementations issues in distributed systems.
3	To understand scheduling in distributed operating systems, process management, fault tolerance, real-time distributed systems, and designing of distributed file systems
4	To study the distributed resource and process management components.
5	To study advanced topics related to distributed operating systems.

INTRODUCTION TO DISTRIBUTED SYSTEMS	**(04 Hours)**
Review of Networking Protocols, Point to Point Communication, Operating Systems, Concurrent Programming, Characteristics and Properties of Distributed Systems, Goals of Distributed Systems, Multiprocessor and Multicomputer Systems, Distributed Operating Systems, Network Operating Systems, Middleware Concept, The Client-Server Model, Design Approaches-Kernel Based-Virtual Machine Based, Application Layering.	
COMMUNICATION IN DISTRIBUTED SYSTEM	**(05 Hours)**
Layered Protocols, Message Passing-Remote Procedure Calls(RPC), Remote Method Invocation(RMI), Message Oriented Communication, Stream Oriented Communication, Case Studies.	
SYNCHRONIZATION IN DISTRIBUTED SYSTEM	**(09 Hours)**
Clock Synchronization, Logical Clocks, Global State, Election Algorithms-The Bully algorithm-A Ring algorithm, Mutual Exclusion- Centralized Algorithm, Distributed Algorithm, Token ring Algorithm, Distributed Transactions, Distributed deadlock detection.	
DISTRIBUTED SHARED MEMORY	**(06 Hours)**
Introduction, General architecture of DSM systems, Design and implementation issues of DSM, Granularity, Structure of shared memory space, consistency models, Replacement strategy, Thrashing.	
RESOURCE MANAGEMENT	**(06 Hours)**
Desirable features of scheduling algorithm, Task assignment approach, Load balancing and Load sharing approach.	
PROCESS MANAGEMENT	**(04 Hours)**
Concept of Threads, Process, Processor allocation, Process Migration and Related Issues, Software Agents, Scheduling in Distributed System, Load Balancing and Sharing Approaches, Fault tolerance, Real time Distributed System	
DISTRIBUTED FILE SYSTEM	**(05 Hours)**
Introduction, Architecture, Mechanisms for Building Distributed File Systems-Mounting-Caching-Hints-Bulk Data Transfer-Encryption, Design issues-Naming and Name Resolution-Caches on Disk or Main Memory-Writing Policy-Cache consistency-Availability-Scalability-Semantics, Case Studies, Log Structured File Systems	
ADVANCED TOPICS	**(04 Hours)**

Introduction of Security in Distributed OS, Overview of security techniques, Features, Need, Access Control, Security Management, Micro Services Architecture, Lockless Data Structures, Distributed/Scalable Messaging Architecture, AMQP.	
CASE STUDY	**(02 Hours)**
Amoeba, Mach, Chorus and their comparison.	
Practical Assignments will be based on the coverage of above topics.	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

List of Practical (Problem Statements will be changed every year and will be notified on Website.)	
1.	Assignments on Client server-based programs using RPC and RMI.
2.	Practical based on Clock Synchronization.
3.	Practical based on Election, Mutual Exclusion and deadlock algorithms.
4.	Programs based on process/code migration.
5.	Assignments based on Case studies.

BOOKS RECOMMENDED

1. Pradeep Sinha, “Distributed Operating Systems Concepts and Design”, 1st ed., PHI Learning Private Limited, 1998.
2. Andrew Tannebaum, “Distributed Operating Systems” 2nd ed., Pearson, 2013.
3. MukeshSinghal, Niranjan G. Shivaratri, "Advanced Concepts in Operating Systems: Distributed, Database, and Multiprocessor Operating Systems", TMGH, 2011.
4. George Coulouris, Jean Dollimore,TimKindberg ,“Distributed Systems: Concepts and Design”, 5th ed., Pearson, 2017.
5. Andrew Tanebaum, Maarten Steen, “Distributed Systems: Principles and Paradigms”, 2nd Ed.

ADDITIONAL BOOKS RECOMMENDED

1. Sunita Mahajan, Seema Shah, “Distributed Computing”, 2nd ed., Oxford University Press, 2013.

Course Outcomes **At the end of the course, students will**	
CO1	gain clear understanding of fundamental principles of Distributed Operating Systems along with design and implementation of key mechanisms, Clock Synchronization, Election Algorithms, Mutual Exclusion, Message Communication, Process and Resource Scheduling etc.
CO2	be able to apply knowledge of various distributed algorithms for real world problems.
CO3	be able to analyze different advanced architectures.
CO4	be able to evaluate different security techniques for distributed problems.
CO5	be able to design various real life applications using principles and paradigms of Distributed Operating System.

M. Tech. I (CSE) Semester – I	**L**	**T**	**P**	**C**
CSCS111: COMPUTER VISION AND IMAGE PROCESSING (CORE ELECTIVE-1 OR 2)	**3**	**0**	**2**	**4**

Course Objective	
1	To understand the fundamentals image processing and computer vision about image formation, representation and camera calibration.
2	To study various image processing operations and computer vision techniques for camera calibration, depth, motion, stereo and optical flow estimation.
3	To learn different vision based advanced techniques for image understanding and interpreting the images in spatial and frequency domain.
4	To learn different feature extraction and algorithm evaluation techniques for image analysis.
5	To enable student to develop various applications using image processing and computer vision techniques.

LOW LEVEL IMAGE PROCESSING	**(08 Hours)**
Overview of Image and Vision Applications, Illumination, Sampling and Quantization, Image representation and Modeling, Image sources, Image processing application, Image Enhancement, Contrast, Resolution, Histogram Equalization, Spatial Filters, Frequency Representation and Filters, Edge detection, Canny edge detector, Corner detection, Morphological Operation, Color Image Processing, Human eye and cognitive aspects of color, Color transformation.	
HIGH LEVEL IMAGE PROCESSING	**(09 Hours)**
Order statistic filters, Image Segmentation, Object Boundary Detection and Representation, Texture representation, Gabor filters, Noise Removal, Blurring, Image restoration, Image compression.	
IMAGE FORMATION AND RADIOMETRY	**(06 Hours)**
Basics of Image Formation and Radiometry, Bidirectional Reflection Distribution Function, Reflectance Map, Image Formation and Coordinate Transformations, Camera Pin-hole model, Camera calibration, Camera Parameters: Internal and External, Camera Parameters estimation, 3D coordinates and transformation.	
SHAPE AND MOTION ANALYSIS	**(06 Hours)**
Calculus of variation theory, Light at Surfaces, Phong Model, Albedo estimation, Horn-Schunk Optical Flow Formulation, Motion estimation, Epipolar geometry, Photometric Stereo, Structure from motion, Depth from stereo, Shape from Shading, Surface smoothness, Relaxation methods for depth estimation, Shape from texture, 3-D models, Volumetric representation and modeling, Surface modeling.	
IMAGE ANALYSIS AND UNDERSTANDING	**(09 Hours)**
Multi resolution approach, Super resolution, MRF based modeling, Labelling, MRF based applications: Segmentation, Object recognition, Facial detection, Biometric: Iris and Finger print, Feature extraction, Feature vector dimension Reduction, Template based modeling for recognition, Knowledge representation, Feature matching algorithm.	
APPLICATIONS	**(07 Hours)**
Video summarization, In-painting, Biometric recognition, Target detection and tracking, Face recognition, Human gesture and action recognition, Animated Character, Rendering.	
Practical and mini-projects will be based on the coverage of the above topics.	**(30 Hours)**
	(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)

List of Practical (Problem Statements will be changed every year and will be notified on Website.)	
1	Implementation of low level, mid-level, and high-level image processing algorithms.
2	Implementation of various filters and transformation techniques for frequency domain operations.
3	Implementation of camera calibration and estimation of internal and external parameters.
4	Implementation of depth using optical flow, stereo and motion.
5	Implementation of application-basedmini-project.

BOOKS RECOMMENDED

1. Rafael C. Gonzales and Richard E. Woods, "Digital Image Processing", 4th edition Education, Reprint 2018.
2. Anil K. Jain, "Fundamentals of Digital Image Processing", PHI, EEE, 4th reprint 2002.
3. David A. Forsyth and Jean Ponce, "Computer Vision: A Modern Approach", Prentice -Hall, 2004.
4. J. R. Parker, " Algorithms for Image Processing and Computer Vision", 2ndedition ,Wiley, 2010.
5. Robert M. Haralick and Linda G. Shapiro, "Computer and Robot Vision ", Addison Wesley, 1992.

ADDITIONAL BOOKS RECOMMENDED

1. Milan Sonka, Vaclav Hlavac, Roger Boyal, “Image Processing Analysis and Machine Vision” 3rdEd. PWS / Thomson Publishing, 2007.
2. Richard Hartley and Andrew Zisserman, “Multiple View Geometry in Computer Vision”, Second Edition, Cambridge University Press, March 2004.

Course Outcomes **At the end of the course, students will**	
CO1	be able to understand fundamentals of image processing and computer vision and image analyzing techniques.
CO2	be able to apply various image processing operations for analyzing images and vision related techniques for segmentation, visualization of depth and camera calibration.
CO3	be able to analyze the problem and effectively use appropriate technique for image processing and vision related problem solving.
CO4	be able to evaluate critically the solutions developed for image processing and vision problems.
CO5	be able to build new applications using advanced image processing and computer vision techniques.

M.Tech. I (CSE) Semester – I	L	T	P	C
CSCS113: ADVANCED DATABASE MANAGEMENT SYSTEMS (CORE ELECTIVE-1 OR 2)	**3**	**0**	**2**	**4**

Course Objective	
1	Enhanced the knowledge in the areas of database management that go beyond traditional (relational) database management systems.
2	Comprehend the query processing efficient information management for Distributed, Parallel and Object Oriented DBMS
3	To understand and implement of web-enabled applications with different programming languages.
4	To enhance the knowledge about spatial data storage and management
5	To understand storage and management issues of the unstructured data.

DISTRIBUTED DATABASE CONCEPTS	**(06 Hours)**
Overview of client - server architecture and its relationship to distributed databases, Concurrency control Heterogeneity issues, Persistent Programming Languages, Object Identity and its implementation, Clustering, Indexing, Client Server Object Bases, Cache Coherence.	
PARALLEL DATABASES	**(06 Hours)**
Parallel Architectures, performance measures, shared nothing/shared disk/shared memory based architectures, Data partitioning, Intra-operator parallelism, Pipelining, Scheduling, Load balancing	
QUERY PROCESSING	**(06 Hours)**
Index based, cost estimation, Query optimization: algorithms, Online query processing and optimization, XML, DTD, XPath, XML indexing, Adaptive query processing.	
ADVANCED TRANSACTION MODELS	**(06 Hours)**
Savepoints, Sagas, Nested Transactions, Multi Level Transactions. Recovery: Multilevel recovery, Shared disk systems, Distributed systems 2PC, 3PC, replication and hot spares, Data storage, security and privacy Multidimensional K- Anonymity, Data stream management.	
MODELS OF SPATIAL DATA	**(05 Hours)**
Conceptual Data Models for spatial databases (e.g. pictogram enhanced ERDs), Logical data models for spatial databases: raster model (map algebra), vector model, Spatial query languages, Need for spatial operators and relations, SQL3 and ADT. Spatial operators, OGIS queries	
WEB ENABLED APPLICATIONS	**(06 Hours)**
Review of 3-tier architecture - Typical Middle-ware products and their usage. Architectural support for 3 -tier applications: technologies like RPC, CORBA, COM. Web Application server - WAS architecture Concept of Data Cartridges - JAVA/HTML components. WAS	
OBJECT ORIENTED DATABASES	**(05 Hours)**
Notion of abstract data type, object oriented systems, object oriented db design. Expert databases: use of rules of deduction in data bases, recursive rules.	
ADVANCE TOPICS	**(05 Hours)**
No SQL Databases, Unstructured Databases, Couchbase, MongoDB, Cassendra, Redis, Memcached.	
Practical and mini-projects will be based on the coverage of the above topics.	**(30 Hours)**
	(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)

BOOKS RECOMMENDED

1. R. Elmasri and S. Navathe, Fundamentals of Database Systems, Benjamin- Cummings 98 Edition 5th Edition, 2007.
2. AviSilberschatz, Hank Korth, and S. Sudarshan, Database System Concepts, McGraw Hill Edition 5th Edition, 2005
3. S. Shekhar and S. Chawla, Title Spatial Databases: A Tour, Prentice Hall, Edition 2003
4. Hector Garcia-Molina, Jeff Ullman, and Jennifer Widom, Database Systems, Pearson Edition 2nd Edition
5. Mattison, Rob Mattison, "Web Data Warehousing and Knowledge Management", MGH.

Course Outcomes **At end of the course Student will be able to**	
CO1	understand advanced database techniques for storing a variety of data with various database models.
CO2	to apply various database techniques/functions with Object Oriented approach to design database for real life scenarios.
CO3	Analyse the problem to design database with appropriate database model.
CO4	Evaluate methods of storing, managing and interrogating complex data.
CO5	Develop web application API’s, Distributed databases with the integration of various programming languages.

M. Tech. I (CSE) Semester – I	**L**	**T**	**P**	**C**
CSCS115: HIGH PERFORMANCE COMPUTING (CORE ELECTIVE-1 OR 2)	**3**	**0**	**2**	**4**

Course Objective	
1	To understand fundamentals concepts related to High-Performance Computing and state-of-the-art in Parallel Programming environment
2	To study the architectures of several types of high-performance computers and the implications on the performance of algorithms of these architectures
3	To provide an in-depth analysis of design issues in parallel computing
4	To learn the programming constructs required for parallel programming
5	To learn how to achieve parallelism in CUDA architectures

PARALLEL PROCESSING CONCEPTS	**(10 Hours)**
Levels of parallelism (instruction, transaction, task, thread, memory, function), Models (SIMD, MIMD, SIMT, SPMD, Dataflow Models, and Demand-driven Computation etc.), Architectures: N-wide superscalar architectures, multi-core, multi-threaded, performance file systems, GPU systems, performance clusters.	
DESIGN ISSUES AND CHALLENGES IN PARALLEL COMPUTING	**(10 Hours)**
Synchronization, Scheduling, Job Allocation, Job Partitioning, Dependency Analysis, Mapping Parallel Algorithms onto Parallel Architectures, Performance Analysis of Parallel Algorithms, Bandwidth Limitations, Latency Limitations, Latency Hiding/Tolerating Techniques and their limitations, Power-Aware Computing and Communication, Power-aware Processing Techniques, Power-aware Memory Design, Power-aware Interconnect Design, Software Power Management.	
PARALLEL PROGRAMMING WITH OPENMP AND MPI	**(10 Hours)**
Programming languages and programming-language extensions for HPC, Inter-process communication, Synchronization, Mutual exclusion, Basics of parallel architecture, Parallel programming with OpenMP and (Posix) threads, Message passing with MPI, Thread Management, Workload Manager, Job Schedulers.	
PARALLEL PROGRAMMING WITH CUDA	**(10 Hours)**
Processor Architecture, Interconnect, Communication, Memory Organization, and Programming Models in high-performance computing architectures: (Examples: IBM CELL BE, Nvidia Tesla GPU, Intel Larrabee Microarchitecture and Intel Nehalem microarchitecture), Memory hierarchy and transaction-specific memory design, Thread Organization, OpenCL.	
ADVANCED TOPICS	**(05 Hours)**
Petascale Computing, Optics in Parallel Computing, Quantum Computers.	
Practical and mini-projects will be based on the coverage of the above topics.	**(30 Hours)**
	(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)

List of Practical (Problem statements will be changed every year and will be notified on the website.)	
1	Implement parallel programming preliminary examples.

2	Implement algorithms using OpenMP and MPI.
3	Implement experiments using CUDA.
4	Implement and evaluate performance HPC algorithms for load distribution, thread management and job scheduling.
5	Implementation of mini-projects in different areas.

BOOKS RECOMMENDED

1. John L. Hennessy and David A. Patterson "Computer Architecture -- A Quantitative Approach", 4th Ed., Morgan Kaufmann Publishers, 2017, ISBN 13: 978-0-12-370490-0.
2. Barbara Chapman, Gabriele Jost and Ruud van der Pas, "Using OpenMP: portable shared memory parallel programming", The MIT Press, 2008, ISBN-13: 978-0-262-53302-7.
3. Marc Snir, Jack Dongarra, Janusz S. Kowalik, Steven Huss-Lederman, Steve W. Otto, David W. Walker, "MPI: The Complete Reference", Volume2, The MIT Press, 1998, ISBN: 9780262571234.
4. Pacheco S. Peter, "Parallel Programming with MPI", Morgan Kaufman Publishers, 1992, Paperback ISBN: 9781558603394.
5. Shane Cook, CUDA Programming: A Developer's Guide to Parallel Computing with GPUs, Morgan Kaufmann publishers, 2014, ISBN: 9780124159334.

Course Outcomes **At the end of the course, students will**	
CO1	learn concepts, issues and limitations related to parallel computing.
CO2	be able to understand and explain different parallel models of computation, parallel architectures, interconnections and various memory organizations in modern high-performance architectures.
CO3	be able to map algorithms onto parallel architectures for parallelism.
CO4	be able to analyze and evaluate the performance of different architectures and parallel algorithms.
CO5	be able to design and implement parallel programs for shared-memory architectures and distributed-memory architectures using modern tools like OpenMP and MPI, respectively.

M. Tech. I (CSE) Semester – I	**L**	**T**	**P**	**C**
CSCS117: FOUNDATIONS OF DATA SCIENCE (CORE ELECTIVE-1 OR 2)	**3**	**0**	**2**	**4**

Course Objective	
1	To understand the fundamentals of data analytics, distributed database, foundational skills in data science, including preparing and working with data; abstracting and modeling.
2	To go from raw data to a deeper understanding of the patterns and learn to store, manage, and analyze unstructured data structures within the data, to support making predictions and decision making.
3	To learn processing large data sets using Hadoop and make predictions using machine learning and statistical methods.
4	To learn computational thinking and skills, various text analysis and stream data analysis techniques including the Python programming language for analyzing and visualizing data.
5	To learn various topics such as statistics, crawling data, data visualization, advanced databases, complex data represented using graphs or high dimensional data and cloud computing, along with a toolkit to use with data.

INTRODUCTION	**(06 Hours)**
Overview of Data Science and Big Data, Datafication: Current landscape of Perspectives, Skill Sets needed; Matrices, Matrices to Represent Relations Between Data and Linear Algebraic Operations on Matrices, Approximately Representing Matrices by Decompositions, SVD and PCA; Statistics: Descriptive Statistics: Distributions and Probability, Statistical Inference: Populations and Samples, Statistical Modeling, Fitting a Model, Hypothesis Testing, Introduction to R and Python.	
DATA PREPROCESSING	**(08 Hours)**
Types of Data and Representations, Acquiring Data, Crawling, Parsing Data, Data Manipulation, Data Wrangling, Data Cleaning, Data Integration, Data Reduction, Data Transformation, Data Discretization, Distance Metrics, Evaluation of Classification, Methods: Confusion Matrix, Student's T-tests and ROC Curves, Exploratory Data Analysis, Basic Tools: Plots, Graphs and Summary Statistics of EDA, Philosophy of EDA.	
GRAPH	**(09 Hours)**
Different Types of Graphs, Trees, Basic Concepts Isomorphism and Subgraphs, Multi Graphs and Euler Circuits, Hamiltonian Graphs, Chromatic Numbers, Graph and Tree Processing Algorithms, Graph based Applications	
DATA VISUALIZATION	**(06 Hours)**
Data visualization: Basic Principles and Tools, Graph Visualization, Data summaries, Link analysis, Mining of Graph, High Dimensional Clustering, Recommendation Systems.	
PARADIGMS FOR LARGE SCALE DATA PROCESSING	**(08 Hours)**
MapReduce, Hadoop System, Software Interfaces, e.g., Hive, Pig, Traditional Warehouses vs. MapReduce Technology, Distributed Databases, Distributed Hash Tables, Near-real-tips Query.	
TEXT ANALYSIS	**(08 Hours)**
Data Flattening, Filtering, Chunking, Feature Scaling, Dimensionality Reduction, Nonlinear Futurization, Shingling of Documents, Locality-Sensitive Hashing for Documents, Distance Measures, LSH Families for Other Distance Measures, Collaborative Filtering, Sampling Data in a Stream, Filtering Streams, Counting Distinct Elements in a Stream, Moments, Windows, Clustering for Streams.	
Practical will be based on the coverage of the above topics.	**(30 Hours)**

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

List of Practical (Problem statements will be changed every year and will be notified on the website.)	
1	Practical related to Hadoop Installation and implementations using artificial data.
2	Introduction to software tools for data analytics science.
3	Practical based on Basic Statistics and Visualization.
4	Practical related to data preprocessing and data preparation for various Data mining processes.
5	Practical related to different SQL and NOSQL databases.
6	Practical based on Classification.
7	Practical based on K-means Clustering.
8	Practical related to Big Text analysis.

BOOKS RECOMMENDED

1. Joel Grus, “Data science from scratch”, O'Reilly Media.
2. Avrim Blum, John Hopcroft, and Ravindran Kannan, “Foundations of Data Science”, Cambridge University Press.
3. Anand Rajaraman and Jeffrey David Ullman, “Mining of Massive Datasets”, Cambridge University Press.
4. Peter Bruce, Andrew Bruce, ”Practical Statistics for Data Scientists: 50”, O’Reilly publishing house.
5. Douglas C. Montgomery and George C. Runger, “Applied statistics and probability for engineers”, John Wiley & Sons.

ADDITIONAL BOOKS RECOMMENDED

1. Jiawei Han, Micheline Kamber and Jian Pei, “Data Mining: Concepts and Techniques”, Morgan Kaufmann.
2. Mohammed J. Zaki and Wagner Miera Jr, “Data Mining and Analysis: Fundamental Concepts and Algorithms”, Cambridge University Press.
3. Matt Harrison, “Learning the Pandas Library: Python Tools for Data Munging, Analysis, and Visualization, O'Reilly.
4. Tom White, ”Hadoop: The Definitive Guide”, O’Reilly Media.

Course Outcomes **At the end of the course, students will**	
CO1	be able to understand the principles and purposes of data science, and articulate the different dimensions of the area.
CO2	be able to apply various data pre-processing and manipulation techniques including various distributed analysis paradigms using Hadoop and other tools.
CO3	be able to apply basic data mining machine learning techniques to build a classifier or regression model, and predict values for new examples.
CO4	be able interpret various large datasets by applying Data Mining techniques like clustering, filtering, factorization.
CO5	be able to implement and perform advanced statistical analysis to solve complex and large dataset problems for real life applications.

M. Tech. - I (CSE) Semester – I	**L**	**T**	**P**	**C**
CSCS119: EMBEDDED SYSTEMS DESIGN (CORE ELECTIVE-1 OR 2)	**3**	**0**	**2**	**4**

Course Objective	
1	To learn about hardware and software design requirements of embedded systems, the processes, methodologies, fundamental problems, and best practices associated with the development of applications in the context of high-performance embedded computing systems.
2	To study several different styles of processors used in embedded systems, the use of interrupts and inter-process communication, techniques for tuning the performance of a processor, and to optimize embedded CPUs.
3	To understand memory system optimizations and the back end of the compilation process to determine the quality of code.
4	To study the importance of embedded multiprocessors, their architectures, design techniques, methodologies, algorithms, IoT, and its applications.
5	To learn various embedded software development tools and provide in-depth knowledge of scheduling algorithms and middleware architectures for multiprocessors and hardware/software co-design and co-synthesis algorithms.

INTRODUCTION: EMBEDDED HARDWARE	**(04 Hours)**
Introduction to embedded systems Hardware needs; typical and advanced, timing diagrams, memories (RAM, ROM, and EPROM) Tristate devices, Buses, DMA, UART and PLD's Built-ins on the microprocessor, Example applications, Design methodologies, Embedded Systems Design flows, Models of computation, Parallelism and computation, Reliable system design, CE architecture.	
INTERRUPTS	**(04 Hours)**
Interrupts basics ISR; Context saving, shared data problem. Atomic and critical section, Interrupt latency.	
SOFTWARE AND OS	**(04 Hours)**
Survey of software architectures, Round Robin, Function queue scheduling architecture, Use of real time operating system, RTOS, Tasks, Scheduler, Shared data reentrancy, priority inversion, mutex binary semaphore and counting semaphore, Parallel execution mechanisms, Superscalar, SMID and Vector processors, Variable performance CPU architectures, CPU Simulation, Automated CPU Design.	
INTER-PROCESS COMMUNICATION	**(05 Hours)**
Inter task communication, message queue, mailboxes and pipes, timer functions, events Interrupt routines in an RTOS environment.	
EMBEDDED COMPUTING	**(07 Hours)**
Embedded design process, System description formalisms, Instruction sets- CISC and RISC, DSP processors, Embedded computing platform- CPU bus, Memory devices, I/O devices, interfacing, designing with microprocessors, debugging techniques, Hardware accelerators- CPUs and accelerators, Accelerator system design, Embedded system software design using an RTOS Hard real-time and soft real-time system principles, Task division, need of interrupt routines, shared data.	
INTERNET OF THINGS	**(05 Hours)**
Introduction, IoT work flow, IoT Protocols: HTTP, CoAP, MQTT, 6 LoWPAN, building IoT applications.	
TOOLS	**(06 Hours)**

Embedded Software development tools. Host and target systems, cross compilers, linkers, locators for embedded systems. Getting embedded software in to the target system, Debugging techniques like JTAGS, Testing on host machine, Instruction set emulators, logic analyzers In-circuit emulators and monitors.	
NETWORK	**(05 Hours)**
Distributed embedded architectures, Networks for embedded systems, Network-based design, and Internet enabled systems.	
SYSTEM DESIGN TECHNIQUES	**(05 Hours)**
Design methodologies, Requirements analysis, System analysis and architecture design, Quality assurance.	
Practical Assignments will be based on the coverage of above topics.	**(30 Hours)**
	(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)

List of Practical (Problem Statements will be changed every year and will be notified on Website.)	
1	Implement experiment based on programming of Embedded boards.
2	Implement experiment based on Embedded OS.
3	Implement RTOS and job scheduler with Embedded systems.
4	Implement Embedded computing algorithm and evaluate the performance using different tools.
5	Implement mini projects based on Embedded systems for real applications.

BOOKS RECOMMENDED

1. Mohamed Ali Mazidi, Janice GillispieMazidi, RolinMcKinlay, “The 8051 Microcontroller and Embedded Systems: Using Assembly and C”, 2nd Edition, Pearson Education, 2011.
2. Raj Kamal, “Embedded Systems-Architecture, Programming and Design”, 2/E, TMH, 2007.
3. Jonathan W. Valvano, “Embedded Microcomputer Systems-Real Time Interfacing”, Thomson Learning, 2006.
4. David A. Simon, “An Embedded Software Primer”, 1/E,Pearson Education,2001.
5. Louis L. Odette, “Intelligent Embedded Systems”, Addison-Wesley, 1991.

ADDITIONAL BOOKS RECOMMENDED

1. Wayne Wolf,“High-Performance Embedded Computing: Architectures, Applications, and Methodologies“, Morgan Kaufmann, 2006, ISBN-13: 978-0123694850.
2. Larry L Peterson, “Computer Networks: A Systems Approach”, Morgan Kaufmann, 2007, ISBN-13:978-0123705488.
3. Frank Vahid and Tony Givargis, “Embedded System Design: A Unified Hardware/Software Introduction”, John Wiley, 2002.
4. Marilyn Wolf, “Computers as Components- Principles of Embedded Computing System Design”, Morgan Kaufmann, 2016.
5. Denial D. Gajski , Frank Vahid, “Specification and design Embedded systems”, Prentice Hall; Facsimile edition, 1994.

Course Outcomes **At the end of the course, students will**	
CO1	be able to understand hardware-software requirements, interrupts and inter process communication of embedded systems.
CO2	be able to apply techniques for simulating processors, for tuning the performance of a processor and to optimize embedded CPUs, such as code compression and bus encoding. They will be able to use middleware architectures for dynamic resource allocation in multiprocessors.
CO3	be able to analyze the embedded systems' specifications and develop software programs.
CO4	be able to evaluate related software architectures and tools for embedded Systems and evaluate the quality of code using the back end of the compilation process and be able to characterize embedded applications and target architectures using different models.
CO5	be able to design and develop real time embedded systems using the concepts of RTOS.

M. Tech - I (CSE) Semester – I	L	T	P	C
CSCS121: SPEECH AND AUDIO PROCESSING (CORE ELECTIVE-1 OR 2)	**3**	**0**	**2**	**4**

Course Objective	
1	To learn the basics of digital signal processing, analytical methods and it's different applications
2	To understand fundamentals of speech
3	To learn different speech models and speech processing
4	To learn the design of different filters in spatial and frequency domain for speech processing
5	To develop skills for analyzing and synthesizing algorithms and systems for speech recognition, identification, classification for different applications.

BASICS OF DIGITAL SIGNAL	**(06 Hours)**
Analog vs. Digital Signal, Continuous vs. Discrete Signal, Issues with Analog signal processing, Digital signal transmission, Overview of different applications, Fundamentals of z-transform, Fourier transform, Overview of Digital filters: FIR and IIR, Sampling theorem, Decimation and Interpolation.	
FUNDAMENTALS OF SPEECH	**(05 Hours)**
Speech signal, Digital representation of speech, Speech production and perception, Acoustic modeling, Acoustic tubes and features, Acoustic phonetics, Sound propagation, Phase vocoder, Channel vocoder, Vocal tract functioning, Vocal tract transfer function, Time domain models, Frequency domain representation, Concepts of Subband.	
TIME DOMAIN ANALYSIS	**(08 Hours)**
Short time energy and average magnitude, Short time average zero-crossing rate, Pitch period estimation, Speech and silence discrimination, Short time autocorrelation function, Median smoothing, Quantization, Companding, Adaptive Quantization, Delta modulation, Differential PCM.	
FREQUENCY DOMAIN ANALYSIS	**(10 Hours)**
Short time Fourier representation, Short time analysis, Spectrographic, Spectrum analysis, Complex Cepstrum, Pitch Detection, Formant estimation, Linear predictive analysis, LPC equation, solutions, Frequency domain interpretation of Linear Predictive analysis, Relations between various speech parameters, Applications of LPC parameters, IIR and FIR filters design.	
SPEECH MODELING AND PROCESSING	**(16 Hours)**
Vocabulary, Language Modeling, Hidden Markov Models, Pattern Classification and Recognition, Speech Compression, Speech synthesis, Speech recognition, Speaker identification, Emotion analysis, Language identification, Speech Conversion, Speech processing using Neural Networks, Deep Learning.	
Practical and mini-projects will be based on the coverage of the above topics.	**(30 Hours)**
	(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)

List of Practical (Problem Statements will be changed every year and will be notified on Website.)	
1	Implementation of basic signal transforms like Fourier, Wavelet and others.
2	Implementation of preliminary feature extractions from speech signals.
3	Implementation of time domain analysis techniques and design of different filters.
4	Implementation of frequency domain analysis techniques and design of different filters.
5	Implementation of advanced techniques of modelling for speech processing.
6	Implementation of application based mini project.

BOOKS RECOMMENDED

1. Lawrence R. Rabiner and Ronald W. Schafer, "Theory and Applications of Digital Signal Processing", Pearson, 2011.
2. Lawrence R. Rabiner and Ronald W. Schafer, "Digital Processing of Speech Signals", Pearson, 2009.
3. Lawrence Rabiner, Biing-Hwang Juang, B. Yegnanarayana, "Fundamentals of Speech Recognition", Pearson, 2009.
4. Douglas O'Shaughnessy, "Speech Communications Human and Machines", Institute of Electrical and Electronics Engineers, 2000.
5. Ben Gold and Nelson Morgan, "Speech and Audio Signal Processing", Wiley, 2006.

ADDITIONAL BOOKS RECOMMENDED

1. M. R. Schroeder, "Computer Speech: Recognition, Compression, Synthesis", Springer Series in Information Science,2nd edition 2004.

Course Outcomes **At the end of the course, students will**	
CO1	be able to understand the process of converting the continuous-time signal into digital signal, process it and convert back to continuous-time signal
CO2	be able to apply the different digital filters to design speech processing applications
CO3	be able to analyse the speech in time domain and frequency domain and also able to analyse tools like Fourier transform and z-transform to find a system's frequency response or system's impulse response
CO4	be able to evaluating the performance of a speech processing based systems like speech recognition, speech identification and many more
CO5	be able to design robust and efficient the speech models and speech processing systems

M.Tech. I (CSE) Semester – I	**L**	**T**	**P**	**C**
CSCS123: 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 platform to solve complex problems.
4	To analyse and evaluate suitable cloud paradigm and big data analytics algorithms and techniques to give solution for complex problem.
5	To design and give solution for given problem 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. T. White, “Hadoop: The definite guide”.
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 platform to solve complex problems.
CO4	be able to analyse and evaluate suitable cloud paradigm and big data analytics algorithms and techniques to give solution for complex problem.
CO5	be able to design and give solution for given problem through big data analytics tools and cloud platform.

M.Tech-I (CSE) Semester – I	L	T	P	C
CSCS125: PRINCIPLES OF INFORMATION SECURITY AND PRIVACY (CORE ELECTIVE-1 OR 2)	**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 of the 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: HTTPS, TLS for Secure Internet Communication, S/MIME, PEM, PGP for Secure Email, the SET, TLS, and HTTPS 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. Strenghts 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. Principles of Information Security, By Michael E. Whitman, Herbert J. Mattord, Course Technology Press, 4th edition, 2011
2. Computer Security, by Dieter Gollmann, Wiley, 3rd edition, 2014
3. Principles of Information Systems Security: Texts and Cases, By GurpreetDhillon, John Wiley & Sons, 1st edition, 2006
4. Information Security Management Principles, by Andy Taylor, David Alexander, Amanda Finch, David Sutton, 3rd edition, BCS, The Chartered Institute for IT Publishers, 2020
5. Cyber Security: A practitioner's guide, by David Sutton, BCS, The Chartered Institute for IT Publishers, 2017

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

CO1	Understand 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) Semester – I	**L**	**T**	**P**	**C**
CSCS127: RESEARCH METHODOLOGY IN CSE (CORE ELECTIVE-1 OR 2)	**3**	**1**	**0**	**4**

Course Objective	
1	To understand the basic terminology of research, and 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 it with the existing approach 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 Objectives, 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	to understand the different research methodologies 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, and 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) Semester – I	L	T	P	C
CSCS129: PROBABILISTIC GRAPHICAL MODELS (CORE ELECTIVE-1 OR 2)	**3**	**1**	**0**	**4**

Course Objective	
1	To understand probability, statistics and graph models.
2	To understand different graphical models for solving real time applications in different fields.
3	To be able to learn the design of different types of network based on graphical models.
4	To be able to model problems using graphical models, design inference algorithms, and learn the structure of the graphical model from data.
5	To learn analysis of the problems for developing their solution, correctness and performance using graphs and statistical methods.

INTRODUCTION TO PROBABILITY THEORY	**(06 Hours)**
Random variables and Joint distributions, Marginal distribution, Conditional probability, Expectation and variance, Functions of random variable, Sum of independent random variable, Correlation and regression, Probability Distributions.	
GRAPH THEORY	**(06 Hours)**
Graphs, Different types of Graphs, Isomorphism and Subgraphs, Multigraphs and Euler Circuits, Hamiltonian graphs, Chromatic Numbers, Algorithms for Graphs Processing, Graph representation, Graph Applications.	
GRAPHICAL MODELS	**(09 Hours)**
Directed models: Bayesian network, Undirected model: Markov Random Fields, Dynamic model: Hidden Markov Model, Conditional Independence, Markov Blanket, Factorization, Equivalence, Hybrid Networks, Template based representation.	
INFERENCE IN GRAPHICAL MODELS	**(09 Hours)**
Exact Inference, Belief Propagation, Approximate Inference, Expectation Propagation, Gaussian Belief Propagation, MAP Inference, Sampling - Markov Chain Monte Carlo, Metropolis Hastings, Gibbs, Particle filtering.	
LEARNING IN GRAPHICAL MODELS	**(09 Hours)**
Parameter estimation, Expectation Maximization, Factor Graph, Bayes Ball theorem and D-separation, Hammersley-Clifford theorem, Inference in graphical models, Belief propagation, Viterbi algorithm, Inference, Optimization. MAP Inference, Inference in Hybrid Networks.	
APPLICATIONS BASED ON GRAPHICAL MODELS	**(06 Hours)**
Actions and Decisions, Structured Decision Problems, Graphical models in Network Analysis, Image Processing, Social Network Analysis.	
Practical Assignments will be based on the coverage of above topics.	**(30 Hours)**
	(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)

List of Practical (Problem statements will be changed every year and will be notified on the website.)	
1	Implement graph traversing algorithms.
2	Implement Markov Random Field based applications.
3	Implement Hidden Markov based applications.
4	Implement Bayesian Network based applications.

BOOKS RECOMMENDED

1. Murray R. Spiegel, John J. Schiller and R. Alu Srinivasan, Theory and Problems of Probability and Statistics, 2nd Edition, Tata McGraw-Hill, 2007.
2. D. Koller and N. Friedman, Probabilistic Graphical Models: Principles and Techniques, MIT Press, 2009.
3. F. V. Jensen and T. D. Nielsen, Bayesian Networks and Decision Graphs, Information Science and Statistics, Springer, 2nd Edition, 2002.
4. A. Papoulis and S. U. Pillai, Probability, Random Variables and Stochastic Processes, 4th Edition, Mc-Graw Hill, 2002.
5. Richard E. Neapolitan, “Learning Bayesian Networks, Prentice Hall Series in Artificial Intelligence, 2003.

Course Outcomes **At the end of the course, students will**	
CO1	be able to acquire knowledge about different terminologies of graphs and statistics.
CO2	be able to apply graph-theoretic models to solve problems of connectivity and constraint satisfaction for different problems.
CO3	be able to analyze the problems for developing the solution, its correctness and performance using graphs and statistics methods learned.
CO4	be able to evaluate the solution built using different graph based modeling.
CO5	be able to design an efficient solution using statistical methods and a variety of graphs for real world problems.

M.Tech. I (CSE) Semester – I	**L**	**T**	**P**	**C**
CSCS131: ARTIFICIAL INTELLIGENCE (CORE ELECTIVE-1 OR 2)	**3**	**0**	**2**	**4**

Course Objective	
1	To introduce the basic concepts of Artificial Intelligence (AI), with illustrations of current state of the art research, tools and applications.
2	To understand the basic areas of AI including problem solving, knowledge representation, heuristic, reasoning, decision making, planning and statistical methods.
3	To identify the type of an AI problem and apply it for search inference, decision making under uncertainty, game theory etc.
4	To describe the knowledge representation techniques, strengths and limitations of various state-space search algorithms, and choose the appropriate algorithm.
5	To introduce advanced topics of AI such as planning, Bayes networks, natural language processing and Expert systems.

INTRODUCTION TO AI AND INTELLIGENT AGENTS	**(05 Hours)**
Basic concepts of Intelligence, Scope and View of AI, Applications of AI, Turing Test, Intelligent Behavior, Intelligent Agents, AI Techniques, AI-Problem formulation, AI Applications, Production Systems, Control Strategies.	
PROBLEM SOLVING	**(08 Hours)**
Defining the problems as a State Space Search and Production Systems, Production Characteristics, Production System Characteristics, And issues in the Design of Search Programs, Additional Problems. Informed and uninformed search strategies: Generate-And-Test, Breadth first search, Depth first search, Hill climbing, Best first search, A* algorithm, AO* Algorithm, Iterative Deepening Search, IDA*, Recursive Best First Search, Constraint propagation, Neural, Stochastic, and Evolutionary search algorithms, Constraint Satisfaction and Heuristic Repair, Applications.	
KNOWLEDGE REPRESENTATION AND REASONING	**(07 Hours)**
Knowledge representation - Production based system, Frame based system, Knowledge representation using Predicate logic, Introduction to predicate calculus, Rule based representations, Declarative / Logical formalisms, Knowledge bases and Inference, Reasoning in uncertain environments, Logic-Structured based Knowledge representation, Inference – Backward chaining, Forward chaining, Rule value approach, Fuzzy reasoning – Certainty factors, Bayesian Theory-Bayesian Network-Dempster – Shafer theory, Symbolic Logic under Uncertainty : Non-monotonic Reasoning, Logics for non-monotonic reasoning, Statistical Reasoning : Probability and Bayes Theorem, Certainty factors, Probabilistic Graphical Models, Bayesian Networks, Markov Networks.	
GAME PLAYING AND PLANNING	**(07 Hours)**
Introduction, Example Domain: Overview, MiniMax, Alpha-Beta Cut-off, Refinements, Iterative deepening, The Blocks World, Components of a Planning System, Goal Stack Planning, Nonlinear Planning Using Constraint Posting, Hierarchical PlanniArtificialIntelligenceng, Reactive Systems, Other Planning Techniques, Recent applications.	
MULTI GAME THEORY	**(08 Hours)**

Introduction, Behavioral game theory: Dictator, Ultimatum and trust games, Mixed strategy equilibrium, Bargaining, Dominant solvable games, Coordination games, Signaling and reputation, Types of learning Reinforcement, Belief, Imitation, Stochastic game theory, Evolutionary games and Markov games for multi-agent reinforcement learning, Economic Reasoning and Artificial Intelligence, Designing games: Cooperative games, Voting, Auctions, Elicitation, Scoring rules, Decision Making and Utility Theory, Adaptive decision making, Analyzing games: Combinatorial games, Zero-sum games, General-sum games, Nash Equilibrium, Correlated Equilibrium, Price of anarchy.	
EXPERT SYSTEMS	**(10 Hours)**
Expert Systems – Architecture of Expert Systems, Roles of Expert Systems – Knowledge Acquisition – Meta Knowledge, Heuristics, Typical Expert Systems – MYCIN, DART, XOON, Expert Systems Shells.	
Practical Assignments will be based on the coverage of above topics.	**(30 Hours)**
	(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)

List of Practical (Problem statements will be changed every year and will be notified on the website.)	
1	Introduction to PROLOG programming.
2	Implement Informed and uniformed based search techniques.
3	Implement various algorithms based on game theory.
4	Practical based on fuzzy logic-based application.
5	Practical based on statistical methods.
6	Implement an expert system for real applications.
7	Practical based on multilayer perceptron.
8	Implement neural network-based application

BOOKS RECOMMENDED

1. Stuart Russell and Peter Norvig, “Artificial Intelligence: A Modern Approach”, Third edition, Prentice-Hall, 2009.
2. Nils J. Nilsson, “Artificial Intelligence: A New Synthesis”, Morgan-Kaufmann, 1998.
3. Elaine Rich and Kevin Knight, “Artificial Intelligence”, 2nd Edition, Tata McGraw-Hill, 2003.
4. W. Patterson, ‘Introduction to Artificial Intelligence and Expert Systems’, Prentice Hall of India, 2010.
5. I. Bratko, "Prolog Programming for Artificial Intelligence", 3/E, Addison-Wesley, 2001.

ADDITIONAL BOOKS RECOMMENDED

1. Donald A.Waterman, “A Guide to Expert Systems”, Pearson Education, 1985, ISBN: 0-201-08313-2.
2. David Poole, Alan Mackworth, “Artificial Intelligence: Foundations for Computational Agents”, Cambridge Univ. Press, 2010.
3. J. Han and M. Kamber, “Mining: Data Concepts and Techniques”, 3rd Edition, Morgan Kaufman, 2011.
4. Hastie, Tibshirani, Friedman, “The elements of statistical learning”, second edition, Springer, 2009.

Course Outcomes **At the end of the course, students will**	
CO1	be able to understand foundational principles, mathematical tools, program paradigms and fundamental issues, challenges of artificial intelligence, formal methods of knowledge representation, logic and reasoning.
CO2	be able to apply intelligent agents for artificial intelligence programming techniques, Fuzzy logic for problem solving and semantic rules for reasoning and inference to real world problems.
CO3	be able to analyze and formalize the problem as a state space, graph, design heuristics and select amongst different search or game-based techniques to solve them.
CO4	be able to evaluate the performance of an informed and uninformed search strategies, fuzzy logic, and expert system and connectionist models based systems.
CO5	be able to design the application on different artificial intelligence techniques like heuristic, game search algorithms, fuzzy, expert system and neural network.

M.Tech. I (CSE) Semester – I	**L**	**T**	**P**	**C**
CSCS133: 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", MIT Press, 2015.
3. ZEADALLY S and NafaâJabeur, "Cyber Physical System Design With Senor Networking Technologies", 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) Semester – I	**L**	**T**	**P**	**C**
CSCS135: 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 role of digital evidences 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 evidences 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, Incidence 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, DhananjayKalbande, “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 andSons, 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 evidences.
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 difference evidences 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 (CSE) Semester – II	**L**	**T**	**P**	**C**
CSCS140: MACHINE LEARNING FOR SECURITY **(CORE ELECTIVE-3 OR 4)**	**3**	**0**	**2**	**4**

Course Objectives	
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 TECHNQIUES 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. SumeetDua 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) Semester – I	L	T	P	C
CSCS139: IDENTITY AND ACCESS MANAGEMENT (CORE ELECTIVE-1 OR 2)	**3**	**0**	**2**	**4**

Course Objective	
1	Understand fundamentals around identity, Authentication, Authorization and Access Control
2	Know various types of Access Controls and Access Administration at high level.
3	Student will get to learn how to access risk and its impact on access control.
4	Student will get the knowledge about Access Control Policies, Standards, Procedures.

INTRODUCTION	**(06 Hours)**
Understand the fundamentals of identity, Authentication & Authorization, Introduction to various types of Access Control & Access Administration, Risk Management and mitigation techniques.	
IDENTITY MANAGEMENT LIFE CYCLE	**(08 Hours)**
Identity Management, Digital Identities, Fundamental requirement for identity management, Identity Management Process, Authentication of Users, Authorization, Proofing, Provisioning, Maintenance, and Entitlement, Zero trust architecture	
AUTHENTICATOR MANAGEMENT (TOKENS, SINGLE SIGN-ON), OFFLINE AND DEVICE AUTHENTICATION	**(12 Hours)**
Token information, time-synchronized one-time passwords, mathematical-algorithm based one-time passwords, physical types, disconnected tokens, connected tokens, contactless tokens, Bluetooth and mobile device tokens, smart cards, types of smart card technology, smart card applications, multifactor authentication, dual control, continuous authentication, periodic authentication, time outs, reverse authentication, certificate-based authentication, authorization, access to systems vs. data, network, access control lists/matrix, and directories, SSO risks, SSO implementation: kerberos, Kerberos applications, Kerberos process, Kerberos considerations, Kerberos tools, network ports used during Kerberos authentication.	
ACCESS CONTROLS	**(15 Hours)**
Regulation of Access, Key concerns of Access Control, Mandatory Access Control (MAC), Non-Discretionary Access Control, Discretionary Access Control (DAC), Role-Based Access Control (RBAC), Rule – Based Access Control (RuBAC), Content Dependent, Context-Based, Temporal Isolation (Time Based), Attribute-Based, Separation of Duties, Security Architecture and Models, role hierarchies, constrained user interface (CUI), types of restricted interfaces, view-based access control (VBAC), and VBAC examples, Content-Dependent Access Control (CDAC), and Temperoal isolation (Time-Based) Access Control, Bell-LaPadula confidentiality Model, Biba integrity model, BLP and Biba model comparison, Clark-Wilson integrity model, and additional models, Applications of Access Control Models for IoT- Based Critical Infrastructure.	
ACCESS ADMINISTRATION PROCESS	**(04 Hours)**
Access provisioning, Access monitoring and review, Access termination	
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 O. Orondo, “Identity & Access Management: A Systems Engineering Approach”, Createspace Independent Publisher.
2. Graham Williamson , Kent Spaulding , IlanSharoni , David Yip, Identity Management, MC Press.
3. Shiu-Kai Chin , Susan Beth Older, “Access Control, Security, and Trust: A Logical Approach”, Chapman and Hall/CRC.
4. Dan M Bowers, “Access Control and Personal Identification Systems”, Butterworth-Heinemann.
5. Osmanoglu, Ertem. “Identity and Access Management: Business Performance Through Connected Intelligence”. Netherlands, Elsevier Science, 2013.

Course Outcomes **At the end of the course, students will**	
CO1	be able to understand the fundamentals of identity, Authentication & Authorization, Introduction to various types of Access Control & Access Administration.
CO2	be able to apply the authentication mechanisms to validate the digital identities.
CO3	be able to analyze the authenticator mechanisms and trust architectures.
CO4	be able to evaluate the access control models.
CO5	be able to design the access control models for IoT based applications.

M.Tech-I (CSE) Semester – I	**L**	**T**	**P**	**C**
CSCS141: SOFTWARE SECURITY **(CORE ELECTIVE-1 OR 2)**	**3**	**0**	**2**	**4**

Course Objectives	
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 analysethe 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 vulnerabiliites.
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 linuxfind(), 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 Modelng tools: Whitebiards, Office-suites, Bug-tracking systems, TRIKE, Sea-monster, Elevation-of-privilege, ThreatModeler, 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 use the concepts of information security to prevent security design faults.
CO5	be able to design the new software with the security features builtin rather than reliance on the security software.

M. Tech-II (CSE) Semester – I	**L**	**T**	**P**	**C**
CSCS143: SECURITY AND PRIVACY IN RESOURCE CONSTRAINED ENVIRONMENTS (CORE ELECTIVE-1 OR 2)	**3**	**0**	**2**	**4**

Course Objectives	
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 WSN and the design of the lightweight cyphers 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) Semester – I	**L**	**T**	**P**	**C**
CSCS145: BLOCKCHAIN FUNDAMENTALS AND USE CASES (CORE ELECTIVE-1 OR 2)	**3**	**0**	**2**	**4**

Course Objectives	
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 BLOKCHAIN	**(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, Trustless ness and Immutability of Blockchain Technology, Proof of Work (PoW) and Proof 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 and challenges 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 evaluate security, privacy, and efficiency of a given blockchain use case.
CO5	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.

M.Tech. I (CSE) Semester – I	**L**	**T**	**P**	**C**
CSCS147: NETWORK SECURITY (CORE ELECTIVE-1 OR 2)	**3**	**0**	**2**	**4**

Course Objectives	
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) Semester – I	**L**	**T**	**P**	**C**
CSCS149: MODERN CRYPTOGRAPHY (CORE ELECTIVE-1 OR 2)	**3**	**1**	**0**	**4**

Course Objectives	
1	to discuss the importance of group theory, number theory, and discrete probability with respect to the modern cryptography.
2	to demonstrate the requirements and applications of deterministic and probabilistic algorithms.
3	to develop the ability to model security problems and to write security proofs.
4	to describe fundamental cryptographic primitives including Key Exchange, Digital Signatures, Oblivious Transfer, Public-Key Encryption, Commitment, to evaluate the security in different real-world scenarios.
5	to communicate different computational problems that are important for cryptography such as the 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, and Topics related to Modern 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 be able to

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) Semester – I	**L**	**T**	**P**	**C**
CSCS151: INFORMATION RETRIEVAL (CORE ELECTIVE-1 OR 2)	**3**	**0**	**2**	**4**

Course Objective	
1	To know the concepts of data retrieval system, introduces the basic principles of data storage, processing, and retrieval in terms of the data retrieval system analysis and design.
2	To understand how information is processed within a data retrieval system.
3	To compare and contrast data retrieval models and internal mechanisms.
4	To critically evaluate data retrieval system effectiveness and improvement techniques.
5	To understand the unique features of Internet-based information retrieval.

INTRODUCTION	**(04 Hours)**
Goals and history of Data Retrieval, Significance of Information Retrieval, Impact of the web on Data Retrieval, Applications of Data Retrieval, Basic Data Retrieval System Architecture, Information Retrieval, Relationships between Digital library and IRS, Abstraction, Algorithms, Data Structures, Measure of information systems, Logical Organization, Physical Organization, Components of Information Retrieval Systems, Comparisons among Different Information Systems.	
DATA CONTROL, PRESENTATION AND RETRIEVAL MODELS	**(06 Hours)**
Query, Differences between Documents and Queries, Type of Documents, Document Surrogates, Vocabulary Control, Structure of a Thesaurus, Structural Representation, Overview of Retrieval Models, Probabilistic Models, Ranking based on Language Models, Complex Queries and Combining Evidence, Machine Learning and Data Retrieval, Application-Based Models, Vector Model, Document-term Matrix, Methods for Designing Weights to Terms, Query in the Vector Model, Spatial Representation of a Document in Vector Model, Similarity between a Query and a Document.	
BASIC SEARCHING AND INDEXING	**(06 Hours)**
Simple Tokenizing, Stop-word Removal, Stemming and Lemmatization, Inverted Indices and Files, Sparse Vectors, Positional Postings and Phrase Queries, Spelling Correction, Phonetic Correction, Index Construction, Index Compression, Extracting Index Terms.	
SIMILARITY MEASURE AND AUTOMATIC CLUSTERING APPROACHES	**(05 Hours)**
Data Fusion, Term Association, General Similarity Measures, Similarity Measures in the Vector Retrieval Model, Extended User Profile, Clustering, Classification, Significance of a Clustering Approach in IR, Categorization of Clustering Algorithms, Non-hierarchical Clustering Algorithm, K-means Clustering algorithm, K-means in SPSS, Hierarchical Clustering Algorithm, Hierarchy Cluster in SPSS	
INFORMATION VISUALIZATION	**(06 Hours)**
Visualization Systems, VIBE, DARE, Visual Thesaurus, Inxight, Reveal Things, Tilebars, SQWID, JAIR INFORMATION SPACE, WebMap, Excentric Labeling, Tree Map, LifeLines, Web Brain, NiF Elastic Catalog, Dynamic Diagrams, Health InfoPark.	
EVALUATION IN DATA RETRIEVAL	**(06 Hours)**
Data Retrieval System Evaluation, Standard test Collections, Evaluation of Unranked Retrieval Sets, Evaluation of Ranked Retrieval Results, Assessing Relevance, A Broader Perspective: System Quality and User Utility, Kappa Measure, Grandfield Experimental Study, Evaluations on Benchmark Text Collections, Web Mining, Web Retrieval Model.	
RELEVANCE FEEDBACK AND QUERY EXPANSION	**(06 Hours)**
Framework for Feedback Methods, Explicit Relevance Feedback, Explicit Feedback Through Clicks, Implicit Feedback Through Local Analysis, Implicit Feedback Through Global Analysis, Trends and Research Issues, Recommender systems.	

IMAGE AND INTERNET DATA RETRIEVAL	**(06 Hours)**
Content-based Image Retrieval, Image Feature Description, Order system, Texture, Shape, Characteristics of Image Queries, Image Retrieval systems, Challenge in the Web, Language Distribution, Centralized Architecture, Crawlers, Jargons, Breadth First Approach, Depth First Approach, Crawling Approach, Web Page Ranking, Meta-search, Considerations for Meta-search Engines.	
Practical and mini-projects will be based on the coverage of the above topics.	**(30 Hours)**
	(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)

List of Practical (Problem statements will be changed every year and will be notified on the website.)	
1	Experiments using different platforms for handling the data of different volumes.
2	Experiments for implementing distributed systems for data storage and its retrieval.
3	Experiments of accessing Big-data and developing an exemplary application.
4	Implementation of mini projects in different fields like image processing, web services, natural language processing, information security etc.
5	Comparison and analysis of different retrieval techniques.

BOOKS RECOMMENDED

1. Christopher D. Manning, Prabhakar Raghavan, and Hinrich Schütze, “Introduction to Information Retrieval”, Cambridge University Press.
2. Ricardo Baeza-Yates and Berthier Ribeiro-Neto, “Modern Information Retrieval”, Addition Wesley.
3. Bing Liu, “Web Data Mining”, Springer.
4. Manning D. Christopher, Prabhakar Raghavan, Schütze Hinrich, “Introduction to Information Retrieval”, Cambridge University Press.
5. Stefan Buettcher, Charles L. A. Clarke, Gordon V. Cormack, “Information Retrieval: Implementing and Evaluating Search Engines”, The MIT Press.

ADDITIONAL BOOKS RECOMMENDED

1. Richard K. Belew, “Finding out about--A cognitive perspective on search engine technology and the www”, Cambridge University Press.
2. Soumen Chakrabarti, “Mining the Web”, Morgan-Kaufmann Publishers.
3. David A. Grossman and Ophir Frieder, “Information Retrieval: Algorithm and Heuristics”, Springer.

Course Outcomes **At the end of the course, students will**	
CO1	have knowledge to describe current trends in information retrieval such as information visualization and be familiar with the structure of queries and documents.
CO2	be able to implement techniques for data retrieval systems.
CO3	be able to analyze the different Retrieval Models.
CO4	be able to evaluate the retrieved information based on various parameters.
CO5	be able to design efficient and robust data retrieval for real time applications.

M. Tech. I (CSE) Semester – I	L	T	P	C
CSCS153: BIG DATA ANALYTICS AND LARGE-SCALE COMPUTING (CORE ELECTIVE-1 OR 2)	**3**	**0**	**2**	**4**

Course Objective	
1	To learn the basics of big data, its characteristics, big data management issues, processing and applications with the help of big data platforms and storage models for big data management.
2	To learn the management and analysis of big data using technology like Hadoop, NoSql, MapReduce, PIG & HIVE.
3	To apply the data mining algorithms on big data for scalability of the real time applications.
4	To develop research interest towards advances in data mining by analyzing the available approaches with the help of evaluating parameters.
5	To build big data analytics and management systems with visualization using the latest technology to solve real problems.

INTRODUCTION	**(05 Hours)**
Definition of Big Data, Source of Big Data, Convergence of Key Trends, Unstructured Data, Industry Examples of Big Data, Web Analytics, Fraud and Risk Associated with Big Data, Credit Risk Management, Big Data in Algorithmic Trading, Healthcare, Medicine, Marketing and Advertising, Big Data Technologies, Introduction to Hadoop and Spark, Open Source Technologies, Cloud, Mobile Business Intelligence, Crowd Sourcing Analytics, Inter and Trans Firewall Analytics.	
BIG DATA ANALYTICS	**(06 Hours)**
Big Data Processing: Batch Data Processing and Stream Data Processing, Computing Environments for Big Data Analytics, Implementation of Batch and Real Time Event Processing: Integration of Disparate Data Stores/Data Lake, Mapping Data to the Programming Framework, Connecting and Extracting Data from Storage, Transforming Data for Processing, Querying.	
DISTRIBUTED FILE SYSTEM HADOOP	**(08 Hours)**
Introduction, HDFS Daemons, Different Methods to HDFS Access, Hadoop, Features, Google File System Features, Phases involved in Map Reduce, Architecture, Execution of MapReduce Jobs, Monitoring the progress of job flows, Building Blocks of Hadoop MapReduce. Data format, Analyzing data with Hadoop, Scaling Out, Hadoop Streaming, Hadoop Pipes, Design of Hadoop Distributed File System, MapReduce, HDFS Concepts: Java Interface, Data Flow, Hadoop I/O, Data integrity, Compression, Serialization, Avro, File-based Data Structures, Mahout, Pig, Hive, HBase.	
DISTRIBUTED MACHINE LEARNING	**(08 Hours)**
Review of Machine Learning: Supervised and Unsupervised Learning, Linear algebra; Classification Formulation, Closed Form Solution, Computational Complexity, Grid Search, Computation Storage Communication, Probabilistic Prediction, Backpropagation Graph and Compute Gradients for Model Training, Automatic Differentiation Graph-Level Optimization Parallelization/Distributed Training Data Layout and Distributed Linear Regression and Distributed Logistic Regression, Placement Kernel Optimizations, Memory Optimizations, Distributed Principal Component Analysis, Regularization and Optimization for Training Deep Neural Networks, Sequence Modeling, Federated Learning.	
BIG DATA ANALYSIS WITH MLLIB, SPARKSQL AND GRAPHX	**(06 Hours)**
HBase, Data Model and Implementations, HBase Clients, HBase Examples, Praxis, Cassandra, Cassandra data Model, Cassandra Examples, Cassandra Clients, Hadoop Integration, Hive, Data Types and File Formats, HiveQL Data Definition, HiveQL Data Manipulation, HiveQL Queries, Applications on Big Data Using Pig and Hive, Data Processing Operators in Pig, Fundamentals of ZooKeeper, K-Means Clustering,	

Decision Trees, Random Forests, Recommenders, Table in Spark, Higher Level Declarative Programming, Network Structure, Computing Graph Statistics.	
BIG DATA STORAGE MODELS	**(06 Hours)**
Introduction, NoSQL Databases, Need, Types, Comparison with RDBMS, Architecture and Features of NoSQL Databases: Distributed Hash-table, Key-Value Storage Model, Document Storage Model, Graph Storage Models, Lambda Architecture, Data Ingestion, Design and Provision Compute Resources, Storage Technology, Streaming Units, Configuration of Clusters for Latency and Throughput, Output Visualization.	
SCALABLE ALGORITHMS	**(06 Hours)**
Mining Big Data, Centrality, Similarity, Al-Distances Sketches, Community Detection, Link Analysis, Spectral Techniques, MapReduce, Pig Latin, and NoSQL, Algorithms for Detecting Similar Items, Recommendation Systems, Data Stream Analysis Algorithms, Detecting Frequent Items, Data Ingestion, Storage of Data, Data Transfer, Compute Clusters and Configuration of Design.	
Practical Assignments will be based on the coverage of above topics.	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

List of Practical (Problem statements will be changed every year and will be notified on the website.)	
1	Working with various functions of Hadoop MapReduce.
2	Working with pySpark and RDDs.
3	Regression and classification in Spark.
4	Data analysis with PCA in Spark.
5	Hands-on with MLlib and SparkSQL.
6	Use cases and implementation for Big data management and large scale machine learning algorithms.

BOOKS RECOMMENDED

1. Ron Bekkerman, Mikhail Bilenko, John Langford, “Scaling up Machine Learning: Parallel and Distributed Approaches”, Cambridge University Press.
2. Michael Minelli, Michele Chambers, AmbigaDhiraj, “Big Data, Big Analytics: Emerging Business Intelligence and Analytic Trends for Today's Businesses", Wiley.
3. Michael Berthold, David J. Hand, “Intelligent Data Analysis”, Springer.
4. Tom White, “Hadoop: The Definitive Guide”, O’reilly Media.
5. ArshdeepBahga, Vijay Madisetti, “Big Data Science & Analytics: A Hands on Approach “, VPT.

ADDITIONAL BOOKS RECOMMENDED

1. Edward Capriolo, Dean Wampler, and Jason Rutherglen, “Programming Hive”, O'Reilly.
2. Lars George, “HBase: The Definitive Guide”, O'Reilly.
3. Eben Hewitt, “Cassandra: The Definitive Guide”, O'Reilly.
4. Alan Gates, “Programming Pig”, O'Reilly.
5. Sandy Ryza, Uri Laserson, Sean Owen, Josh Wills, “Advanced Analytics with Spark”, O'Reilly.
6. Holden Karau, Andy Konwinski, Patrick Wendell, and MateiZaharia,Learning Spark, O'Reilly.
7. Jure Leskovec, Stanford Univ.AnandRajaraman, Milliway Labs, Jeffrey D. Ullman, “Mining of Massive Datasets”, Cambridge University Press.
8. Ron Bekkerman, Mikhail Bilenko and John Langford, “Scaling up Machine Learning: Parallel and Distributed Approaches”, Cambridge University Press.
9. Arvind Sathi, “Big Data Analytics: Disruptive Technologies for Changing the Game”, MC Press.
10. Tom Plunkett, Brian Macdonald et al, “Oracle Big Data Handbook”, Oracle Press.
11. Jay Liebowitz, “Big Data and Business analytics”, CRC press.

Course Outcomes **At the end of the course, students will**	
CO1	have knowledge of the key issues in big data management and its associated applications in intelligent business and scientific computing.
CO2	be able to apply theoretical foundations of mining algorithms for the usage applicability of business, engineering and scientific problems for big data processing and scalability.
CO3	be able to analyze Hadoop related tools such as HBase, Cassandra, and Hive for big data analytics.
CO4	be able to evaluate the big data analytics applications and evaluation measures to have a productive solution.
CO5	be able to build a complete business data analytics solution for any real time problem.

M.Tech. I (CSE) Semester – II	**L**	**T**	**P**	**C**
CSCS112: ANN AND DEEP LEARNING (CORE ELECTIVE 3 OR 4)	**3**	**0**	**2**	**4**

Course Objective	
1	To introduce the fundamental techniques and principles of Neural Networks
2	To study the different models in ANN and their applications.
3	To explore in depth deep neural architectures for learning and inference and to evaluate the performance of neural architectures in comparison to other machine learning methods
4	To familiarize deep learning concepts with Convolutional Neural Network case studies
5	To implement the concepts of deep learning algorithms and solve real-world problems.

INTRODUCTION TO ARTIFICIAL NEURAL NETWORKS	**(05 Hours)**
Fundamentals of Neural Networks, Computational models of neurons, Structure of neural networks, Single and multi-layer perceptrons, Learning Methods, Functional units of ANN for pattern recognition tasks, Applications.	
FEEDFORWARD NEURAL NETWORKS	**(06 Hours)**
Pattern classification using perceptron, Multilayer feedforward neural networks, Training Neural Network: Empirical risk minimization, Activation functions, Loss functions, Back propagation learning, Regularization, Model selection and optimization, Auto encoders.	
DEEP NEURAL NETWORKS	**(12 Hours)**
Deep Feed Forward network, Difficulty of training DNNs, Greedy layer wise training, Optimization for training DNNs, Newer optimization methods for neural networks (AdaGrad, RMSProp, Adam), Second order methods for training, Regularization methods: dropout, drop connect, batch normalization.	
CONVOLUTION NEURAL NETWORKS	**(12 Hours)**
Introduction to CNNs – convolution, pooling, Deep CNNs, Different deep CNN architectures – LeNet, AlexNet, VGGNet, GoogLeNet, ResNet. Training CNNs: weights initialization, batch normalization, hyper parameter optimization, Understanding and visualizing CNNs, Applications of CNN– Object Detection, and Content based image Retrieval.	
RECURRENT NEURAL NETWORKS	**(06 Hours)**
Sequence modeling using RNNs, Back propagation through time, Long Short-Term Memory, Bidirectional LSTMs, Bidirectional RNNs, Gated RNN Architecture, Basics of word embedding.	
APPLICATIONS AND TOOLS	**(04 Hours)**
Applications in vision, speech and natural language processing e.g., Image and video captioning along with the use of attention. Deep Learning Tools: Caffe, Theano, Torch.	
Practical Assignments will be based on the coverage of above topics.	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

List of Practical (Problem Statements will be changed every year and will be notified on Website.)	
1	Practical based on single layer and multi-layer feed forward Neural Network.
2	Practical based on different activation functions and loss functions.

3	Practical based on back propagation learning algorithm.
4	Implement trained CNN architectures.
5	Implement object detection task using trained CNN models.
6	Practical based on word embedding.
7	Practical based on LSTM.
8	Practical based on GRU.

BOOKS RECOMMENDED

1. S. Haykin, “Neural Networks and Learning Machines” , Prentice Hall of India, 2010.
2. Ian Goodfellow, YoshuaBengio and Aaron Courville, “Deep learning”, In preparation for MIT Press, 2016.
3. CharuC.Aggarwal “Neural Networks and Deep learning” Springer International Publishing, 2018.
4. Satish Kumar, “Neural Networks - A Class Room Approach”, Second Edition, Tata McGraw-Hill, 2013.
5. Simon Haykin, “Neural Networks, A Comprehensive Foundation”, 2nd Edition, Addison Wesley Longman, 2001.

ADDITIONAL BOOKS RECOMMENDED

1. 1.B. Yegnanarayana, “Artificial Neural Networks”, Prentice- Hall of India, 1999.
2. 2.Bishop, Christopher M. “Pattern Recognition and Machine Learning”. Springer, 2006.
3. 3.Duda R.O., Hart P.E., Stork D.G., “Pattern Classification”, Second edition, Wiley-Interscience, 2001.
4. 4.Russell S., Norvig N., “Artificial Intelligence: A Modern Approach”, Prentice Hall Series in Artificial Intelligence, 2003.

Course Outcomes
At the end of the course, students will

CO1	be able to understand basic Neural Network architectures, key concepts, issues and practices, core algorithms and optimization when training and modeling with deep architectures.
CO2	be able to apply fundamental principles, theory and approaches for learning with deep neural networks.
CO3	be able to analyze main variants of deep learning architectures, their typical applications.
CO4	be able to evaluate the performance of a different Convolution Neural Networks, LSTM and Gated RNN Architecture
CO5	be able to design real world application based on the concepts of ANN and deep learning.

M.Tech. I (CSE) Semester – II	**L**	**T**	**P**	**C**
CSCS114: INTRODUCTION TO FORMAL SPECIFICATION AND VERIFICATION (CORE ELECTIVE 3 OR 4)	**3**	**0**	**2**	**4**

Course Objective	
1	To understand the general concepts of requirements extraction, modelling and specifications.
2	To design the requirements model and specify the requirements using semi-formal techniques viz. Finite State Machines, Communicating Finite State Machines, and Petrinets.
3	To understand the basic concepts in logic specifications and in temporal logic, set theory, and discrete math.
4	To specify the systems using logic specifications and using the Temporal Logic of Actions (TLA+).
5	To verify general safety properties by proofs or TLC model checking tool.
6	To understandsystemcorrectnessasanimportantpartofengineeringethics.

INTRODUCTION	**(02 Hours)**
Functional & Non-functional requirements. Software Qualities the non-functional requirements. Software Requirements Extraction, Modeling and Specifications.	
SOFTWARE VARIFICATION AND VALIDATION	**(07 Hours)**
Approaches to analyse software code. Execution-based and non-execution-based testing. Static analysis. Static analysis using the illustrative tools viz.Splint, FlawFinder, SonarQube, Synopsis's Coverity Scan OR any other static analysis tool. Detection of software vulnerabilities using the gdband Stack analysis.	
SOFTWARE SPECIFICATIONS	**(08 Hours)**
Formal Specifications. Specification definition, types and the uses. Qualities of the Specifications and illustrations of bad specifications. Formal Methods for Verification of Specifications: Semi-Formal Specification techniques viz. Finite State Machines, The Communicating Finite State Machines, Petri nets, Timed Petri nets. Modeling the classical distributed/-concurrent applications viz. the Producer Consumer problem, the Readers Writers problem, the Traffic Lights problem, the Trains tracks shunting problem, the Coffee-Biscuits-Chocolates vending machine problem, the Elevator Controller problem etc. Extending the basic Petrinets.	
MODELLING AND FORMAL VERIFICATION OF DISTRIBUTED APPLICATIONS	**(08 Hours)**
Illustrating the basic theory of Formal Verification. Illustrating modeling with PROMELA through various examples. Modelling distributed applications using Petrinet modeling tool. Specifications using the Alloy, with the Alloy tutorial.	
DECLARATIVE SPECIFICATIONS	**(08 Hours)**
Review of the Propositional Logic and the First Order logic, Inference Rules. Logic specifications, Specifying programs and parts of programs. Specifying Classes and non-terminating behaviours. Logic Specifications case study through the Elevator Controller Problem. Descriptive Specifications, Algebraic specifications and illustrations. Specifications for ADTs like String, Queue, Editors, etc.	
FORMAL SPECIFICATION AND VERIFICATION LANGUAGE	**(12 Hours)**
Temporal Logic of Actions (TLA+). Simple math and TLA specifications. Asynchronous interface specification and TLATeX type setter. Caching memory specifications. Temporal logic: safety and liveness properties TLA+ for program designing, modeling, documentation, and verification. Applications for concurrent systems and distributed systems. Specification and verification of real	

time systems.	
Practical assignments will be based on the coverage of the above topics.	**(30 Hours)**
	(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)

BOOKS RECOMMENDED

1. L. Lamport, Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers. Addison Wesley. 2003. Ghezzi, Jazayeri, Mandrioli: Fundamentals of Software Engg, 2003 ed, Pearson EDU
2. Pankaj Jalote: An integrated approach to SE, Narosa, 3rd edition, ‘05
3. Rajib Mall: Software Engineering, Prentice Hall of India, 4th Edition, 2014.
4. Grumberg, Clarke, Peled: Model Checking, The MIT Press, 2001.
5. Gerard J. Holzmann. Design and Validation Of Computer Protocols (Prentice Hall Software Series). October 1990

Course Outcomes
At the end of the course, students will

CO1	Understand the general concepts of requirements extraction, modeling and specifications.
CO2	be able to specify the systems using logic specifications and using the Temporal Logic of Actions (TLA+).
CO3	Understand the basic concepts in logic specifications and in temporal logic, set theory, and discrete math.
CO4	be able to verify general safety properties by proofs or TLC model checking tool.
CO5	be able to design the requirements model and specify the requirements using semi-formal techniques and using SPIN/PROMELA.

M.Tech. I (CSE) Semester – II	**L**	**T**	**P**	**C**
CSCS116: NATURAL LANGUAGE PROCESSING (CORE ELECTIVE 3 OR 4)	**3**	**0**	**2**	**4**

Course Objective	
1	To comprehend natural language processing in order to extract information.
2	To understand information about language-specific tasks and learning models.
3	To investigate the use of artificial intelligence to comprehend the semantics of text data.
4	To know about text processing at syntactic, semantic, and pragmatic levels.
5	To understand data extraction from unstructured text by identifying references to named entities as well as stated relationships between such entities.

INTRODUCTION AND LANGUAGE MODELING	**(12 Hours)**
Introduction to Computational Linguistics, Word Meaning, Distributional Semantics, Word Sense Disambiguation, Sequence Models, N-gram Language Models, Feed forward Neural Language Models, Word Embedding, Recurrent Neural Language Models, Tokenization, Lemmatization, Stemming, Sentence Segmentation, POS Tagging and Sequence Labeling, Structured Perceptron, Viterbi – Loss, Augmented Structured Prediction, Neural Text Models and Tasks.	
INFORMATION EXTRACTION	**(11 Hours)**
Information Extraction from Text, Sequential Labeling, Named Entity Recognition, Semantic Lexicon Induction, Relation Extraction, Paraphrases Inference Rules, Summarization, Event Extraction, Opinion Extraction, Temporal Information Extraction, Open Information Extraction, Knowledge based Population, Narrative Event Chains and Script Learning, Knowledge Graph Augmented Neural Networks for Natural Language.	
MACHINE TRANSLATION AND ENCODER-DECODER MODELS	**(11 Hours)**
Machine Translation, Encoder-Decoder Models, Beam Search, Attention Models, Multilingual Models, Syntax, Trees, Parsing, Transition based Dependency Parsing, Graph based Dependency Parsing, Transfer Learning, Deep Generative Models for Natural Language Data, Text Analytics, Text Mining, Information Extraction with AQL-Conversational AI.	
APPLICATION AND CASE STUDIES	**(11 Hours)**
Application: Spelling Correction, Sentiment Analysis, Word Sense Disambiguation, Text Classification, Machine Translation, Question Answering System, Intent Detection, False Fact Detection.	
Practical assignments will be based on the coverage of the above topics	**(30 Hours)**
	(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)

List of Practical (Problem statements will be changed every year and will be notified on the website.)	
1	Create an application in Python with the NLTK library to tokenize the words present in a paragraph.
2	Perform tasks with NLTK (Natural Language Toolkit).
3	Tasks to be Performed in SpacCy Library.
4	Practicals based on huggingface library.
5	Text Classification using movie reviews database, etc.
6	Practical implementation of application and case study.

BOOKS RECOMMENDED

1. Emily Bender, “Linguistics Fundamentals for NLP”, Morgan Claypool Publishers.
2. Jacob Eisenstein, “Natural Language Processing”, The MIT Press.
3. Dan Jurafsky, James H. Martin, “Speech and Language Processing”, Prentice Hall.
4. Chris Manning, HinrichSchutze, “Foundations of Statistical Natural Language Processing”, The MIT Press.
5. Pushpak Bhattacharyya, “Machine Translation”, CRC Press.

Course Outcomes **At the end of the course, students will**	
CO1	be able to understand how language works, including the word structure, sentence structure, and meaning.
CO2	be able to learn how to reframe NLP problems as learning and inference tasks, as well as how to deal with the associated computational challenges
CO3	be able to use text processing at the syntactic, semantic, and pragmatic levels.
CO4	be able to learn about text mining and manipulation techniques.
CO5	be able to retrieve information from the text and can use it for decision making.

M.Tech. I (CSE) Semester – II	**L**	**T**	**P**	**C**
CSCS118: REINFORCEMENT LEARNING (CORE ELECTIVE 3 OR 4)	**3**	**0**	**2**	**4**

Course Objective	
1	To learn reinforcement learning as a general framework to design an autonomous decision-making system.
2	To learn how to define RL tasks and the core principals behind the RL, including policies, value functions, deriving Bellman equations.
3	To understand and work with tabular methods to solve classical control problems.
4	To recognize current advanced techniques and applications in RL.
5	To describe (list and define) multiple criteria for analyzing RL algorithms and evaluate algorithms on these metrics: e.g. regret, sample complexity, computational complexity, empirical performance, convergence, etc.

INTRODUCTIONS	**(06 Hours)**
Introduction to Reinforcement Learning, Basics of RL, Defining RL Framework and Markov Decision Process, Polices, Value Functions and Bellman Equations, Exploration vs. Exploitation, Code Standards and Libraries used in RL (Python/Keras/Tensorflow).	
TABULAR METHODS AND Q-NETWORKS	**(08 Hours)**
Planning through the use of Dynamic Programming and Monte Carlo, Tabular MDP planning, Temporal-Difference Learning Methods (TD(0), SARSA, Q-Learning), n-step Bootstrapping, Deep Q-Networks (DQN, DDQN, Dueling DQN, Prioritized Experience Replay), Tabular RL Policy Evaluation.	
FUNCTION APPROXIMATIONS	**(07 Hours)**
Introduction to Function Approximations, Function Approximation with on-policy methods, Non-linear Function Approximation, Function Approximation with off-policy methods, Average Reward RL.	
POLICY GRADIENTS METHODS	**(08 Hours)**
Introduction to Policy-based Methods, Vanilla Policy Gradient, REINFORCE Algorithm and Stochastic Policy Search, Actor-critic Methods (A2C, A3C), Advanced Policy Gradient (PPO, TRPO, DDPG).	
PLANNING AND MODEL-BASED RL	**(08 Hours)**
Model based RL approach, Model Predictive Control, Eligibility Traces, Hierarchical RL, Partial Observability, POMDPs, and Offline RL.	
RECENT ADVANCES AND APPLICATIONS	**(08 Hours)**
Meta-learning, Multi-Agent Reinforcement Learning, Partially Observable Markov Decision Process, Ethics in RL, Applying RL for Real-World Problems.	
Practical will be based on the coverage of the above topics separately.	**(30 Hours)**
	(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)

List of Practical (Problem Statements will be changed every year and will be notified on Website.)	
1	Implementation of RL Framework and Markov Decision Process Model.
2	Implementation of Code Standards and Libraries used in RL.
3	Implementation of Temporal-Difference Learning Methods.
4	Implementation of Deep Q-networks.
5	Implementation of Policy optimization Methods.

BOOKS RECOMMENDED
1. Richard S. Sutton and Andrew G. Barto, "Reinforcement learning: An introduction", Second Edition, MIT Press, 2019. 2. Li, Yuxi. "Deep reinforcement learning." arXiv preprint arXiv: 1810.06339 (2018). 3. Szepesvári, Csaba. "Algorithms for reinforcement learning." Synthesis lectures on artificial intelligence and machine learning 4, no. 1 (2010): 1-103. 4. Russell, Stuart J., and Peter Norvig. "Artificial intelligence: a modern approach. “Pearson Education Limited, 2016. 5. Wiering, Marco A., and Martijn Van Otterlo. "Reinforcement learning." Adaptation, learning, and optimization 12.3 (2012): 729.

Course Outcomes **At the end of the course, students will**	
CO1	have a knowledge of the core challenges in designing RL systems and how to approach them.
CO2	be able to define RL tasks and the core principals behind the RL, including policies, value functions, deriving Bellman equations.
CO3	be able to implement in code common algorithms following code standards and libraries used in RL.
CO4	be able to understand and work with tabular methods to solve classical control problems.
CO5	be able to recognize current advanced techniques and applications in RL.

M.Tech. I (CSE) Semester – II	**L**	**T**	**P**	**C**
CSCS120: DATA MINING AND DATA WAREHOUSING (CORE ELECTIVE 3 OR 4)	**3**	**0**	**2**	**4**

Course Objective	
1	To introduce students to the basic concepts and techniques of Data Mining.
2	To introduce a wide range of association, clustering, estimation, prediction, and classification algorithms.
3	To introduce mathematical statistics foundations of the Data Mining Algorithms.
4	To introduce basic principles, concepts and applications of Data Warehousing.
5	To build a data mining application from a data warehouse to solve real problems.

OVERVIEW	**(05 Hours)**
Introduction, Data Mining Issues, Data Mining Metrics, Data Mining from a Database Perspective, Data Mining Techniques: Classification, Statistical-Based Algorithms, Decision Tree -Based Algorithms, Neural Network-Based Algorithms, Rule-Based Algorithms, Combining Techniques; Similarity and Distance Measures, Hierarchical Algorithms, Partitioned Algorithms, Clustering Large Databases, Clustering with Categorical Attributes; Basic Algorithms, Advanced Association Rule Techniques, Measuring the Quality of Rules	
MINING STREAM, TIME SERIES AND SEQUENCE DATA	**(10 Hours)**
Mining Data Streams, Methodologies for Stream Data Processing and Stream Data Systems, Frequent-Pattern Mining in Data Streams, Classification of Dynamic Data Streams, Clustering Evolving Data Streams; Trend Analysis, Similarity Search in Time Series Analysis, Sequential Pattern Mining in Transactional Databases, Constraint-Based Mining of Sequential Patterns, Periodicity Analysis for Time-Related Sequence Data; Mining Sequence Patterns, Alignment of Sequences, Hidden Markov Model for Sequence Analysis.	
MULTIMEDIA DATA MINING	**(08 Hours)**
Multimedia Data, Similarity Search in Multimedia Data, Multidimensional Analysis of Multimedia Data, Classification and Prediction Analysis of Multimedia Data, Mining Associations in Multimedia Data, Audio and Video Data Mining.	
SPATIAL DATA MINING	**(08 Hours)**
Spatial Data, Mining Spatial Association and Co-location Patterns, Spatial Classification and Spatial Trend Analysis, Spatial Clustering Methods, Mining Raster Databases	
DATA WAREHOUSING	**(08 Hours)**
Review of Data Warehouse, Multidimensional Data Model, Data Cubes, Process Architecture, OLAP Operations, Stream OLAP and Stream Data Cubes, Generalization of Structured Data, Aggregation and Approximation in Spatial and Multimedia Data Generalization, Generalization of Class Composition Hierarchies, Construction and Mining of Object Cubes, Generalization-Based Mining of Plan Databases by Divide-and-Conquer, Spatial Data Cube Construction and Spatial OLAP.	
APPLICATIONS AND OTHER DM TECHNIQUES	**(06 Hours)**
Mining Event Sequences, Visual DM, Data Stream Mining, Multimedia Mining, Spatial Mining.	
Practical assignment will be based on the coverage of the above topics.	**(30 Hours)**
(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)	

List of Practical (Problem statements will be changed every year and will be notified on the website.)	
1	Implementation of an application of a KDD process.
2	Analysis of Data Mining Techniques with Implementations using Java, Python etc.
3	Implementation of Nearest Neighbor Learning and Decision Trees.
4	Analysis of Splitting and Merging Clusters.
5	Implementation of association rule mining algorithms.
6	Mini Project: Implementation of Selected Journal Papers.

BOOKS RECOMMENDED

1. Jiawei Han, MichelineKamber, "Data Mining: Concepts and Techniques", Morgan Kaufman.
2. Ville, "Decision Trees for Business Intelligence and Data Mining: Using SAS Enterprise Miner", SAS.
3. Pang-Ning Tan, Michael Steinbach, Vipin Kumar, "Introduction to Data Mining", Addison Wesley.
4. Tom Soukup, Ian Davidson, "Visual Data Mining: Techniques and Tools for Data Visualization and Mining", Wiley.
5. Alex Berson, Stephen J. Smith, "Data Warehousing, Data Mining, and OLAP", MGH.

Course Outcomes **At the end of the course, students will**	
CO1	be able to identify the key processes of data mining, data warehousing and knowledge discovery process and understand the basic principles and algorithms used in practical data mining.
CO2	be able to apply data mining techniques to solve problems in other disciplines in a mathematical way.
CO3	be able to analyze the algorithms used in practical data mining and their strengths and weaknesses.
CO4	be able to evaluate different strategies of data warehousing techniques and data mining algorithms.
CO5	be able to design data mining algorithms for real time applications.

M.Tech. I (CSE) Semester – II	**L**	**T**	**P**	**C**
CSCS122: DATA SCIENCE FOR SOFTWARE ENGINEERING (CORE ELECTIVE 3 OR 4)	**3**	**0**	**2**	**4**

Course Objective	
1	To understand various tools of Software Engineering.
2	To understand the capability of software engineering principles to analyze data science applications to make appropriate decisions.
3	To learn various methods and principles of software engineering for data science applications.
4	To learn integration of software engineering principles with data science applications.
5	To learn how to use software engineering for data science.

FORMAL SOFTWARE ENGINEERING	**(06 Hours)**
Formal specifications, Techniques, Verification and Validation, Theorem Provers, Model checking, modeling concurrent systems, Temporal logics, CTL & LTL and model checking, SAT Solvers, Testing Techniques, Test Case Generation	
SOFTWARE REQUIREMENTS AND ESTIMATION	**(04 Hours)**
Software Requirements: What and Why, Software Requirements Engineering, Software Requirements Management, Software Requirements Modeling, Software Estimation, Size Estimation, Effort, Schedule and Cost Estimation, Tools for Requirements Management and Estimation.	
SOFTWARE DEVELOPMENT METHODOLOGIES	**(05 Hours)**
Introduction to Software Engineering, A Generic View of Process, Process Models, Software Requirements, Design Engineering, Creating an Architectural Design, Modeling Component.	
SOFTWARE PROCESS AND PROJECT MANAGEMENT	**(05 Hours)**
Software Process Maturity, Process Reference Models, Software Project Management Renaissance, Life-Cycle Phases and Process artifacts, Workflows and Checkpoints of Process, Process Planning, Project Organizations, Project Control and Process Instrumentation, CCPDS-R Case Study and Future Software Project Management Practices.	
FUNDAMENTALS OF OBJECT ORIENTED DESIGN IN UML	**(05 Hours)**
Static and Dynamic Models, Necessity of Modeling, UML Diagrams, Class Diagrams, Interaction Diagrams, Collaboration Diagram, Sequence Diagram, State Chart Diagram, Activity Diagram, Implementation Diagram.	
USER INTERFACE	**(04 Hours)**
Module Introduction, Objectives of Usability, How to Approach Usability, Designing with Usability in mind, Measuring Usability, Guidelines for User Interface Design, User Interface Elements.	
SOFTWARE QUALITY ASSURANCE AND TESTING	**(04 Hours)**
Software Quality Assurance and Standards, Quality Standards, Software Testing Strategy and Environment, Building Software Testing Process, Software Testing Techniques, Software Testing Tools, Testing Process-Seven Step Testing Process, Specialized Testing Responsibilities.	
DATA SCIENCE PERSPECTIVE FOR SOFTWARE ENGINEERING	**(12 Hours)**
Diverse Sets of Data, Category of Data, Combining Quantitative and Qualitative Methods, Structuring and Summarizing Unstructured Software Data, Validate and Calibrate Data, Generation of Requirement Specifications, Automatic Code Documentation; Software Project Cost Estimation, Software Quality Prediction, Semi-Automatic Refactoring, Prioritization, Automatic Bug Assignment and Test Cases Generation; Case Study-Search Engine: Working of Search Engine, Content Quality Strategy, Control Crawling, Indexing and Ranking, Search Appearance, Optimization.	

Practical Assignments will be based on the coverage of above topics.	**(30 Hours)**
	(Total Contact Time: 45 Hours + 30 Hours = 75 Hours)

List of Practical (Problem statements will be changed every year and will be notified on the website.)	
1	Working with software engineering software SPIN.
2	Working with a variety of modules for software engineering.
3	Working with testing of the software project.
4	To develop the software engineering prototype of the application.
5	To analyze the software using a model checker.

BOOKS RECOMMENDED

1. Roger S. Pressman, “Software Engineering: A Practitioner's Approach”, McGraw Hill Higher Education.
2. Ian Sommerville, “Software Engineering”, Pearson Education.
3. Carlo Ghezzi, Mehdi Jazayeri, Dino Mandrioli, “Fundamentals of Software Engineering”, Pearson.
4. Hans van Vliet, “Software Engineering: Principles and Practice”, Wiley.
5. Tim Menzies, Laurie Williams, Thomas Zimmermann, “Perspectives on Data Science for Software Engineering”.

Course Outcomes **At the end of the course, students will**	
CO1	have knowledge about software engineering tools for integrated development environments, syntax checking, testing, debugging, and version control.
CO2	be able to apply software engineering principles to solve Data Science applications.
CO3	be able to critically analyze the Data Science problems to apply software engineering solutions.
CO4	be able to evaluate various Data Science applications using software engineering principles.
CO5	be able to design software engineering principles based applications using Data Science principles.

M.Tech. I (CSE) Semester – II	L	T	P	C
CSCS124: SECURITY AND PRIVACY IN SOCIAL NETWORKS (CORE ELECTIVE 3 OR 4)	**3**	**0**	**2**	**4**

Course Objectives	
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 ofan 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.	
Advance 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 algorithm 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) Semester – II	L	T	P	C
CSCS126: FOUNDATIONS OF PRIVACY ENGINEERING (Core Elective 3 or 4)	**3**	**1**	**0**	**4**

Course Objectives	
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 the 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) Semester – II	**L**	**T**	**P**	**C**
CSCS128: MALWARE ANALYSIS AND MITIGATION (CORE ELECTIVE 3 OR 4)	**3**	**0**	**2**	**4**

Course Objective	
1	To identify and describe common traits of malware.
2	To examine and analyse malwares using static and dynamic analysis techniques.
3	To apply different tools for malware detection.
4	To evaluate potential threats due to malware activity on system or network.
5	To create malware analysis report from studied technique and develop mitigation strategies.

INTRODUCTION	**(08 Hours)**
Introduction To Malwares, Different Types of Malwares, Characteristics of Malwares.	
STATIC ANALYSIS	**(12 Hours)**
Identification and Initial Assessment of Malwares, Antivirus Scanning, Hashing, Finding Strings, Packed and Obfuscated Malware, File Formats, Linked Libraries and Functions, X86 Architecture and Disassembly, Recognizing C Code Constructs In Assembly, Analyzing Malicious C Programs, Shellcode Analysis	
DYNAMIC ANALYSIS	**(08 Hours)**
Sandboxes, Process Monitors, Process Explorer, Registry Snapshots, Faking A Network, Packet Sniffing, Source and Assembly Level Debugger, Kernel and User Level Debugging, Exceptions.	
MALWARE FUNCTIONALITY	**(08 Hours)**
Malware Behaviour, Covert Malware Launching, Data Encoding, Malware Focused Network Signatures	
ANTI REVERSE ENGINEERING	**(09 Hours)**
Anti-Disassembly, Anti-Debugging, Anti-Virtual Machine Techniques, Packers and Unpacking	
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 Sikorski, andrewHonig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software publisher William Pollock, 2012.
2. Michael Hale Ligh, andrew Case, Jamie Levy, AAron Walters, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, 2014.
3. Ligh, M., Adair, S., Hartstein, B., Richard, M., “Malware analyst's cookbook and DVD: tools and techniques for fighting malicious code”, Wiley Publishing, 2010.
4. Marak V., “Windows malware analysis essentials”, Packt Publishing Ltd, 2015.
5. Dang, B., Gazet, A., Bachaalany, E., “Practical reverse engineering: x86, x64, ARM, Windows kernel, reversing tools, and obfuscation”, John Wiley & Sons, 2014.

Course Outcomes At the end of the course, students will	
CO1	have the knowledge of different types of malware, its behavior and analysis techniques.
CO2	be able to apply different tools and techniques for malware data acquisition and analysis.
CO3	be able to analyse the effect of malware on system and network.
CO4	Be able to evaluate potential threats due to malware activity on system or network.
CO5	be able to create malware analysis report and suggest suitable preventive measures.

M.Tech. I (CSE) Semester – II	**L**	**T**	**P**	**C**
CSCS130: 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 analysethe 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 the 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 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 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 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 LANGAUGES & 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 linuxfind(), 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 Modelng 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 onthe 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”.
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. Malcolm McDonald, “Web Security for Developers: Real Threats”, Practical Defense by

ADDITIONAL BOOKS RECOMMENDED

1. Steven Palmer, “Web Application Vulnerabilities: Detect, Exploit, Prevent by”.
2. IzarTarandach, “Threat Modeling: A Practical Guide for Development Teams”.
3. Tanya Janca, “Alice and Bob Learn Application Security”.

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) Semester – II	L	T	P	C
CSCS132: MOBILE SECURITY AND PENETRATION TESTING (CORE ELECTIVE 3 OR 4)	3	0	2	4

Course Objectives	
1	to understand the importance of security issues in the 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 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, Thedrozer 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 Andriod Applications: Setting up the target app. Analzing 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	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 use the concepts of information security to prevent security design faults.
CO5	be able to design the threat models and security mis-use case diagrams to model the security threats the software being developed.

M.Tech. I (CSE) Semester – II	**L**	**T**	**P**	**C**
CSCS134: BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES (CORE ELECTIVE 3 OR 4)	**3**	**0**	**2**	**4**

Course Objectives	
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 analyze 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.

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) Semester – II	**L**	**T**	**P**	**C**
CSCS136: SECURITY PROTOCOLS **(CORE ELECTIVE 3 OR 4)**	**3**	**0**	**2**	**4**

Course Objectives	
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 inMurphi, 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 forthe 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) Semester – II	**L**	**T**	**P**	**C**
CSCS138: HARDWARE SECURITY (CORE ELECTIVE 3 OR 4)	**3**	**0**	**2**	**4**

Course Objectives	
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, PCBintegrity 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 RajatSubhra 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) Semester – II	**L**	**T**	**P**	**C**
CSCS172: SOCIAL NETWORKS (INSTITUTE ELECTIVE)	**3**	**0**	**0**	**3**

Course Objectives	
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 the social network research solutions for real-world scenarios
CO4	be able to evaluate different methods for social network representation and analytics.
CO5	be able to design the social network analytics solution for the complex real-world problem.

M.Tech. I (CSE) Semester – II	**L**	**T**	**P**	**C**
CSCS174: CYBER LAWS (INSTITUTE ELECTIVE)	**3**	**0**	**0**	**3**

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 & loop holes 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.	

CYBER SPACE JURISDICTION	**(06 Hours)**
Cyber Space 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.	
	(Total Contact Time: 45 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**	
CO1	be able to understand the types of Crime in Internet, Crimes targeting Computers and Scope of Cyber Laws.
CO2	be able to apply the cyber laws to related the various evidences of cybercrimes.
CO3	be able to analyze the various evidences of cybercrimes to allied with the particular cyber law.
CO4	be able to evaluate the particular intellectual property rights according to the cyber law.
CO5	be able to design an application to counter the cybercrimes.

M.Tech. I (CSE) Semester – II	**L**	**T**	**P**	**C**
CSCS176: ETHICAL HACKING AND PENETRATION TESTING (INSTITUTE ELECTIVE)	**3**	**0**	**2**	**4**

Course Objectives	
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 Scannning: 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 a 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, user names 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. ErdalOzkaya, “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; 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. Michael Sikorski, Andrew Honig, “Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software”, Format: Kindle Edition.

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 foot printing including stealth scanning.
CO3	be able to analyze the installations for the vulnerabilities that could be exploited by an adversary.
CO4	be able to extend the existing tools for network and systems protection.
CO5	be able to design the secure system installations that can withstand the adversarial attacks.

M.Tech-I (CSE) Semester – II	L	T	P	C
CSCS178: MACHINE LEARNING (INSTITUTE ELECTIVE)	**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 apply different concepts for the machine learning problems
3	To apply and analyze different supervised and unsupervised learning approaches as per the suitability of the problem
4	To understand and evaluate machine learning methods to use them
5	To design solution of problem using different machine learning approaches

INTRODUCTION	**(05 Hours)**
Pattern Representation, Concept of Pattern Recognition, Basics of Probability, Bayes’ Decision Theory, Maximum-Likelihood and Bayesian Parameter Estimation, Error Probabilities, Learning of Patterns, Modeling, Regression, Discriminant Functions, Linear Discriminant Functions, Decision surface, Learning Theory, Fisher Discriminant Analysis.	
LINEAR ALGEBRA FOR ML	**(06 Hours)**
SUPERVISED LEARNING ALGORITHMS	**(06 Hours)**
Gradient Descent, Linear Regression, Support Vector Machines, K-Nearest Neighbor, Naïve Bayes, Bayesian Networks, Classification, Decision Trees, ML and MAP Estimates, Overfitting, Regularization, Bayes Classification, Nearest Neighbor Classification, Cross Validation and Attribute Selection, Bayesian Decision Theory, Losses and Risks, Bayesian Networks, Parametric Methods: Gaussian Parameter Estimation, Maximum Likelihood Estimation, Bias and Variance, Bayes' Estimator, Bayesian Estimation, Parametric Classification, Regression, Naive Bayes, Hidden Markov Models, Support Vector Machines, Decision Trees.	
NEURAL NETWORKS AND LEARNING ALGORITHMS	**(06 Hours)**
Artificial Neural Networks, Perceptron, Multilayer Networks, Back Propagation, Deep Neural Networks, Convolutional Neural Networks, Recurrent Neural Networks; Linear Discrimination, Multilayer Perceptrons: Multilayer Perceptrons, Backpropagation Algorithm, Nonlinear Regression, Convergence, Overtraining, Dimensionality Reduction, Gradient Descent, Recurrent Networks, Cross-Validation and Resampling Methods, Bootstrapping.	
UNSUPERVISED LEARNING ALGORITHMS	**(06 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, Nonparametric techniques for density estimation, Parzen-window method.	
MISCELLANEOUS TOPICS	**(06 Hours)**
Dimensionality Measuring Error, Interval Estimation, Hypothesis Testing, Reduction, Feature Selection, Principal Component Analysis, Pattern Analysis using Eigen Decomposition, Principal Component Analysis, Parzen-windows Method, Model Selection and Theory of Generalization, In-sample and Out-of-sample Error, Vapnik-Chervonenkis (VC) Dimension, VC Inequality, VC Analysis.	
APPLICATIONS	**(10 Hours)**

Signal Processing, 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 Edition, 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 Taylor and NelloCristianini, “Kernel methods for pattern analysis” Cambridge university press, 2004.

ADDITIONAL BOOKS RECOMMENDED

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

Course Outcomes **At the end of 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.