**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, MIT Manipal**

# M.Tech. COMPUTER SCIENCE AND INFORMATION SECURITY

**Program Structure (Applicable to 2019 admission onwards)**

| YEAR | FIRST SEMESTER | | | | | | SECOND SEMESTER | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | SUB CODE | SUBJECT NAME | L | T | P | C | SUB CODE | SUBJECT NAME | L | T | P | C |
| I | MAT 5152 | COMPUTATIONAL METHODS AND STOCHASTIC PROCESSES | 4 | 0 | 0 | 4 | CSE 5271 | CRYPTANALYSIS | 3 | 1 | 0 | 4 |
| | HUM 5151 | RESEARCH METHODOLOGY AND TECHNICAL COMMUNICATION | 1 | 0 | 3 | 2 | CSE 5256 | ADVANCED MACHINE LEARNING | 3 | 1 | 0 | 4 |
| | CSE 5151 | ADVANCED COMPUTER NETWORKS | 3 | 1 | 0 | 4 | CSE **** | ELECTIVE I | 4 | 0 | 0 | 4 |
| | CSE 5152 | ADVANCED DATA STRUCTURES AND ALGORITHMS | 3 | 1 | 0 | 4 | CSE **** | ELECTIVE II | 4 | 0 | 0 | 4 |
| | CSE 5153 | ADVANCED DATABASE SYSTEMS | 3 | 1 | 0 | 4 | CSE **** | ELECTIVE III | 4 | 0 | 0 | 4 |
| | CSE 5171 | ADVANCED CRYPTOGRAPHY | 3 | 1 | 0 | 4 | *** **** | OPEN ELECTIVE | 3 | 0 | 0 | 3 |
| | CSE 5162 | PROGRAM LAB | 0 | 0 | 3 | 1 | CSE 5262 | INFORMATION SYSTEMS LAB II | 0 | 0 | 6 | 2 |
| | CSE 5163 | INFORMATION SYSTEMS LAB I | 0 | 0 | 6 | 2 | | | | | | |
| | **Total** | | **17** | **4** | **12** | **25** | | | **21** | **2** | **6** | **25** |
| | THIRD AND FOURTH SEMESTER | | | | | | | | | | | |
| **II** | CSE 6098 | PROJECT WORK | | | | | | | **0** | **0** | **0** | **25** |

| PROGRAM ELECTIVES | | OPEN ELECTIVES | |
|---|---|---|---|
| CSE 5005 | COMPUTER VISION & IMAGE PROCESSING | CSE 5051 | DEEP LEARNING |
| CSE 5254 | FUNDAMENTALS OF QUANTUM COMPUTING | CSE 5052 | SOFTWARE PROJECT MANAGEMENT AND QUALITY ASSURANCE |
| CSE 5013 | SYSTEM AND NETWORK SECURITY | | |
| CSE 5014 | CYBER FORENSICS | | |
| CSE 5015 | BLOCKCHAIN TECHNOLOGY AND APPLICATIONS | | |
| CSE 5016 | CYBER LAW AND ETHICS | | |
| CSE 5017 | DATA HIDING | | |
| CSE 5018 | DATABASE AND APPLICATION SECURITY | | |
| CSE 5019 | DISTRIBUTED AND CLOUD SECURITY | | |
| CSE 5020 | HARDWARE SECURITY | | |
| CSE 5021 | INFORMATION SECURITY MANAGEMENT | | |
| CSE 5022 | INTERNET OF THINGS SECURITY | | |
| CSE 5023 | MOBILE AND WIRELESS SECURITY | | |
| CSE 5024 | SECURE SOFTWARE DESIGN | | |

## SEMESTER I

## MAT 5152 COMPUTATIONAL METHODS AND STOCHASTIC PROCESSES [4 0 0 4]

Random variables, one and two dimensional random variables, expectation, variance, covariance and correlation coefficient of random variables, uniform distribution, Functions of random variables, Bayesian estimation, credible intervals, Bayesian Hypothesis. Statistics of stochastic processes, Stationarity; Autocorrelation, Power density spectrum. Markov Models, Gaussian mixture models. Data Analysis, Regression, Predicting real value outputs. Optimization Techniques**,** Mathematical formulation of linear programming problems, Simplex method. Numerical solution to BVP's by finite difference & finite element methods. Solution of parabolic elliptic, hyperbolic PDEs. Linear Algebra, several decompositions and Singular Value decomposition (SVD). Basics of Graph theory, connectivity, spanning tree and traversability. Two person zero sum game theory, non- zero sum game theory. Dominance Method, Graphical Method.

**References:**

1. A. Papoulis and S.U. Pillai, Probability, Random Variables and Stochastic Processes, McGraw Hill, 2002.
2. P. Z. Peebles Jr., Probability, Random Variables and Random Signal Principles, McGraw Hill International Edition, 2001, Singapore.
3. Applied Numerical Methods McGraw Hill.
4. Hamdy A.Taha – Operations Research McGraw Hill.
5. Frank Harary, Graph Theory, Narosa Publishing House 2001.
6. David C Lay, Linear Algebra and its Applications, Pearson Publications (Third Edition).
7. Narsingh Deo, Graph Theory with Applications to Engg. and Computer Science, PHI Learning Private Ltd

**Course Outcomes**

By the end of the course student should be able to:

CO1: Use the improved logical skills of linear algebra.

CO2: Apply probability theory in network and control theory.

CO3: Use probability related concepts in stochastic process , stochastic graph and Makov models.

CO4: Solve engineering problems by numerical methods.

CO5: Solve optimization problems using simplex method.

CO6: Apply the concept of game theory in engineering applications

## HUM 5151 RESEARCH METHODOLOGY AND TECHNICAL PRESENTATION [1 0 3 2]

Mechanics of Research Methodology: Basic concepts: Types of research, Significance of research, Research framework, Case study method, Experimental method, Sources of data, Data collection using questionnaire, Interviewing, and experimentation. Research formulation: Components, selection and formulation of a research problem, Objectives of formulation, and Criteria of a good research problem. Research hypothesis: Criterion for hypothesis construction, Nature of hypothesis, need for having a working hypothesis, Characteristics and Types of hypothesis, Procedure for hypothesis testing, Sampling methods- Introduction to various sampling methods and their applications. Data Analysis: Sources of data, Collection of data, Measurement and scaling technique, and Different techniques of Data analysis. Thesis Writing and Journal Publication: thesis writing, journal and conference papers writing, IEEE and Harvard styles of referencing, Effective Presentation, Copyrights, and avoiding plagiarism.

The Lab focusses on enabling students to develop experiments, analyze data, think critically about theory and data and communicate their results and analysis in writing and oral presentation.

**References**

1. Dr Ranjit Kumar, Research Methodology: A Step-by-Step Guide for Beginners, SAGE, 2005.
2. Geoffrey R. Marczyk, David DeMatteo & David Festinger, Essentials of Research Design and Methodology, John Wiley & Sons, 2004.
3. John W. Creswel , Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, SAGE, 2004
4. Suresh C. Sinha and Anil K. Dhiman, Research Methodology (2 Vols-Set), Vedam Books, 2006.
5. C. R. Kothari, Research Methodology: Methods and Techniques, New Age International Publisher, 2008.
6. Donald R Cooper & Pamela S Schindler , Business Research Methods, McGraw Hill International, 2007.
7. R. Pannershelvam, Research Methodology, Prentice Hall, India, 2006
8. Manfred Max Bergman, Mixed Methods Research, SAGE Books, 2006.
9. Paul S. Gray, John B. Williamson, David A. Karp, John R. Dalphin, The Research Imagination, Cambridge University press, 2007.
10. Cochrain & Cox, Experimental Designs, II Edn. Wiley Publishers, 2006

**Course Outcomes**

After completing the course, the student will be able to:

CO1: Define concept of research and recall types of research.
CO2: Define the problem and develop the research design to solve the problem.
CO3: Organize a thesis report and a manuscript.
CO4: Develop effective technical presentation.
CO5: Develop a good research proposal

## CSE 5151 ADVANCED COMPUTER NETWORKS [3 1 0 4]

Unmanned aerial vehicle(uav) networks: Introduction, challenges, key issues, comparative study, UAV features, Multi-UAV network, UAV network topologies, categorization, self-organization in UAV networks, UAV routing protocols, Handoffs in UAV networks. SDN: Benefits, Use cases, Controllers, Policies, Overlays, Automating Cloud via SDN. Supporting Multivendor Ecosystems. Data Center Evolution: Modern Data Center, Monolithic Storage Array, Virtualization, Convergence, the Role of Cloud, Cloud Types, Cloud Drivers. Emerging Data Center Trends, Hyperconverged Infrastructure. Multimedia Networking: Types of Multimedia, Streaming, DASH. CDN, Case Studies. VoIP. Best-Effort Service, Jitter, Best-Effort Networks, QoS Guarantees, Resource Reservation, Call Admission**.** Optical Networks: Multiplexing, Generations, Switching, Transparency. WDM Network Elements: Optical Line Terminals, Amplifiers, Multiplexers, OADM Architectures. Network Survivability: Basic Concepts, Self-Healing rings, Protection, Resilient Packet Rings, Service Classes.

**References:**

1 https://nptel.ac.in/courses/106105160/18 (Accessed on 2/2/2019).

2. Brian Underdahl and Gary Kinghorn, "*Software Defined Networking For Dummies*", Cisco Special Edition, John Wiley & Sons, Inc., 2015.

3. Scott D. Lowe, James Green, and David Davis, "*Building a Modern Data Center: Principles and Strategies of Design*", ActualTech Media, USA, 2016.

4. James F. Kurose, Keith W. Ross, "*Computer Networking-A Top Down Approach*", (6e), Pearson, 2013.

5. Rajiv Ramaswami, Kumar N. Sivarajan, Galen H. Sasaki, "*Optical Networks -A Practical Perspective*", (3e), Morgan Kaufmann, 2010.

6. Relevant research papers.

**Course Outcomes**

After completing the course, the student will be able to:

CO1: Analyse different UAV routing protocols.

CO2: Identify SDN usecases and recognize SDN controllers.

CO3: Identify different types of Data Centers.

CO4: Analyse and apply different multimedia networking techniques.

CO5: Recognize WDM network elements and network survivability.

## CSE 5152 ADVANCED DATA STRUCTURES AND ALGORITHMS [3 1 0 4]

Amortized Analysis: Aggregate analysis, The Aggregate analysis, The accounting method, The potential method, Dynamic Tables. B-Trees,: Basic operations on B-Trees, Deleting a key from a B-Tree. Binomial trees and Binomial heaps: Operations on Binomial heaps. Structure of Fibonacci heaps, Mergeable heap operations, Decreasing a key and deleting a node. The van Emde Roas Tree: Preliminary approaches, A recursive structure, Disjoint-set operations: Linked-list representation of disjoint sets, Disjoint set forests. Single-Source Shortest Path: The Bellman-Ford algorithm, Single-source shortest paths in directed acyclic graphs, Difference constraints and shortest paths. All-Pairs Shortest Paths: shortest Paths and matrix multiplication, Johnson's algorithm for sparse graphs. Maximum Flow: Flow Networks, The Ford-Fulkerson method, Maximum Bipartite Matching, Multithreaded Algorithms: The basics of dynamic multithreading, Multithreaded matrix multiplication , Multithreaded merge sort.

**References:**

1. Cormen Thomas H., Leiserson Charles E, Rivest Ronald L. and Stein Clifford, *"Introduction to* Algorithms", (3e), MIT Press, 2009.
2. Cormen Thomas H., Leiserson Charles E, Rivest Ronald L. and Stein Clifford, "*Introduction to Algorithms"* (2e), Prentice-Hall India, 2001.
3. Baase Sara and Gelder A.V., "Computer Algorithms -Introduction to Design and Analysis", (3e), Pearson Education, 2000
4. Anany Levitin, "Introduction to the Design and Analysis of Algorithms ", (3e), Pearson Education, 2011

### Course Outcomes

After completing the course, the student will be able to:

CO1: Perform sequence of different types of data structure operations and their cost finding techniques

CO2: Learn various advanced data structures such as B-tree, Binomial heaps, Fibonacci heaps

CO3: Identify to find the use of disjoint sets and when to use van Emde Roas Tree.

CO4: Discover shortest paths for all pairs of vertices and from single source to all other vertices.

CO5: Understand the concept of maximum flow networks and to design and analyze Multi-Threading algorithms.

## CSE 5153 ADVANCED DATABASE SYSTEMS [3 1 0 4]

Introduction to Distributed Data Processing, Top-Down Design Process, Distributed Design Issues, Fragmentation, Allocation, Data Directory, Data Access Control, Complexity of Relational Algebra Operations, Characterization of Query Processors, Layers of Query Processing Properties of Transactions, Types of Transactions, Serializability Theory, Locking-Based Concurrency Control Algorithm, Timestamp-Based Concurrency Control Algorithm, Dead lock Management, “Relaxed” Concurrency Control, Reliability Concepts, Failures in Distributed DBMS, Local Reliability Protocols, Distributed Reliability Protocols, Consistency of Replicated Databases, Replication Protocols, Group Communication, Replication and Failures, Replication Mediator Service, NoSQL: Aggregate Data Models, Distribution Models, Consistency, Version Stamps, Map Reduce, Polyglot Persistence

**References:**

1. M. Tamer Ozsu, Patrick Valduriez, *“Principles of Distributed Database Systems”, (3e), Springer, 2011*
2. Pramod J. Sadalage, Martin Fowler, “*NoSQL Distilled: A Brief Guide to the Emerging World of Polyglot Persistence’, (1e), Person Education, Inc., 2013.*
3. Saeed K. Rahimi and Frank S, Haug, *“Distributed Database Management Systems: A Practical Approach”, (1e), John Wiely & Sons, 2010*
4. Martin Kleppmann, “*Designing Data-Intensive Applications: The Big Ideas Behind Reliable, Scalable, and Maintainable Systems*”, (1e), O’Reilly Media,Inc., 2017
5. Guy Harrison,*“Next Generation Databases: NoSQL, NewSQL and BigData*”, (1e), Apress, 2015

### Course Outcomes

After completing the course, the student will be able to:

CO1: Understand the concepts of Distributed Database Systems (DDBSs), its Design issues and View Management.

CO2: Analyse the techniques in Distributed Query Processing and Optimization.

CO3: Evaluate problems with Transactions Management and Concurrency Control in a Distributed system.

CO4: Use the different protocols to handle Reliability and Replication in DDBSs.

CO5: Evaluate and apply NoSQL Data Models for Data Intensive Applications.

## CSE 5171 ADVANCED CRYPTOGRAPHY [3 1 0 4]

Groups, rings, Fields, Characteristic of a field, prime fields, Arithmetic of polynomials over fields. Field extensions, Galois group of field extensions, Fixed field and Galois extensions. Minimum polynomial, Splitting field of a polynomial, Separable polynomial and Separable extensions. Construction of finite fields and their structure. Enumeration of irreducible polynomials over finite fields. The fundamental theorem of Galois Theory. ElGamal Cryptosystem, Elliptic Curve Architecture, and Cryptography: Elliptic Curve over real numbers, Elliptic Curve Cryptography, ECDH, ECDSA. RSA variants. Authentication functions, Message Authentication Codes and systems, Advanced Digital signature systems. Entity Authentication, One-time password, Challenge – Response: using a symmetric- key cipher, using keyed-hash functions, using as an asymmetric-key cipher, using a digital signature, Zero-Knowledge proof, Fiat. -Shamir protocol, Feige-Fiat-Shamir protocol, Guillou-Quisquater protocol, Biometric, Key Management: Symmetric key distribution, servers. the symmetric key agreement, Deffie-Hellman key agreement, Station to station key agreement. public key distribution, public announcements, certification authority, public key infrastructure, trust model, hijacking.

**References:**

1. Behrouz A. Forouzan and Debdeep Mukhopadhyay – “Cryptography and Network Security”, McGraw Hill, 2nd Edition, 2008.
2. S. Vaudenay, “A Classical Introduction to Cryptography: Applications for Communications Security”, Springer International Edition, 2006.
3. Lawrence C. Washington, “Elliptic curves: number theory and cryptography”, Chapman & Hall/ CRC Second Edition, 2008.
4. William Stallings,“Cryptography And Network Security Principles And Practice”, Fifth Edition, Pearson Education, 2013

**Course Outcomes**

After completing the course, the student will be able to:

CO1: Describe the principles of number theory for cryptography

CO2: Apply number theory concepts in cryptographic algorithms

CO3: Analyse the various hashing algorithms

CO4: Compare the various digital signature schemes

CO5: Demonstrate the concepts of entity authentication and key management

## CSE 5162 PROGRAM LAB [0 0 3 1]

This lab will provide a platform for students to strengthen their programming skills and enhance their understanding of the application of the various language elements. In the latter half of this lab, students will enhance their problem-solving skills by building solutions to more complex problems.

## CSE 5163 INFORMATION SYSTEMS LAB-I [0 0 6 2]

Experiments based on theory covered in Advanced Database Systems, Advanced Computer Networks and Number Theory and Cryptography. In the latter half of this lab, students will be working on more complex problems.

## SEMESTER II

## CSE 5271 CRYPTANALYSIS [3 1 0 4]

Historical cryptanalysis, Preliminaries, Security, attacks on modern block and stream ciphers**,** Correlation attacks, Algebraic attacks, Brute force cryptanalysis, Dictionary attacks, Brute force attacks, Attacks on public key cryptosystems, Eratosthenes's sieve, Improvements, Finding primes faster: Atkin and Bernstein's sieve, Birthday attacks, Analysis of birthday paradox bounds, Finding collisions, Pohlig-Hellman algorithm, Baby-step, giant-step algorithm, Birthday-based algorithms, Analysis of random functions, - Pollard's Rho factoring algorithm , Pollard's Rho discrete logarithm algorithm ,Pollard's kangaroos A direct cryptographic application in the context of blockwise security, Collisions in hash functions , Birthday attack on Plain RSA and plain ElGamal encryptions, Birthday attack on plain ElGamal , The elliptic curve factoring method- Pollard's p-1 factoring, quadratic sieve, Discrete logarithms with the Gaussian integer method, Attacks on hash functions, Constructing number field sieve polynomials, A linear model of SHA, Searching for collision instances.

**References:**

1. Antoine Joux, "*Algorithmic Cryptanalysis"*, CRC Press, 2009
2. Gregory V. Bard, "*Algebraic Cryptanalysis"*, Springer, 2009.
3. Richard J Spillman, "Classical and Contemporary Cryptology", Pearson Education, 2005.
4. Hans Delfs and Helmut Knebl, "Introduction to Cryptography: Principles and Applications", Springer- Verlag, 2007.
5. Alfred John Menezes, Paul C. van Oorschot, Scott A. Vanstone "Handbook of Applied Cryptography", CRC Press, 1996.

**Course Outcomes**

After completing the course, the student will be able to:

CO1: Analyse the various attacks on block and stream ciphers.

CO2: Compare the various algorithms for solving factorization problem, discrete logarithm problem and sieve algorithms to break the public key cryptosystems.

CO3: Demonstrate the attacks on hash functions using birthday paradox and brute force methods.

CO4: Apply the birthday based functions for cryptanalysis.

CO5: Explain elliptic curve factoring methods and number sieve algorithms for cryptanalysis.

## CSE 5256 ADVANCED MACHINE LEARNING [3 1 0 4]

Well-posed learning problems, designing a learning system, concept learning as search, Feature extraction, and feature selection. Metric and Non-Metric Proximity Measures, Modified KNN, Fuzzy KNN, Decision boundaries, Discriminate Functions, univariate and multivariate parameter estimations. Efficient Nearest Neighbour Classifier: Branch and bound, cube, projection, ordered partion, Minimal Distance Classifiers: centroid, condensed. Data organization, Hierachical, Agglomerative, Divisive and partition clustering, Fuzzy K-means, Incremental clustering: Leader, Birch, CF-tree, Model selection for latent variable models and evolutionary algorithms. Entropy and information gain estimation techniques, splitting attribute procedure, Random Forest decision tree representation. Appropriate problems for neural network learning, Multilayer network and the back propagation algorithm for classification of unconstrained document images. KSOM Algorithms, Radial basis functions. Conditional Independence, Parameter estimation, Minimum error-rate classification, Minimum error rate, discriminant functions. Ensemble models.

**References:**

1. Machine Learning – Tom M. Mitchell, - MGH, 2013.
2. Richard o. Duda, Peter E. Hart and David G. Stork, pattern classification, John Wiley & Sons Inc., 2001.
3. Ethem Alpaydin, “Introduction to Machine Learning”, Prentice Hall of India, 2005
4. Stephen Marsland, “Machine Learning –An Algorithmic Perspective”, CRC Press, 2009

**Course Outcomes**

After completing the course, the student will be able to:

CO1: Understand principles and overview of learning problems domains and algorithms.

CO2: Apply learning techniques like random-forest, clustering, and SOM models.

CO3: Apply text classification-based Bayes models for problem solving.

CO4: Understand probability learning, Fuzzy KNN, RBF, based machine learning systems

CO5: Apply and understand evalutionary algorithms and multi expert learning systems

## CSE 5262 INFORMATION SYSTEMS LAB-II [0 0 6 2]

Experiments based on theory covered in Secure Software Design and System and Network Security. In the latter half of this lab, students will be working on more complex problems.

## SECOND YEAR

### CSE 6098 PROJECT WORK [0 0 0 25]

Students are required to undertake innovative and research oriented projects, which not only reflect their knowledge gained in the previous two semesters but also reflects additional knowledge gained from their own effort. The project work can be carried out in the institution/ industry/ research laboratory or any other competent institutions. The duration of project work should be a minimum of 36 weeks. There will be a mid-term evaluation of the project work done after about 18 weeks. An interim project report is to be submitted to the department during the mid-term evaluation. Each student has to submit to the department a project report in prescribed format after completing the work. The final evaluation and viva-voice will be after submission of the report. Each student has to make a presentation on the work carried out, before the departmental committee for project evaluation. The mid-term & end semester evaluation will be done by the departmental committee including the guides.

## ELECTIVES

### CSE 5005 COMPUTER VISION & IMAGE PROCESSING [4 0 0 4]

INTRODUCTION: Introduction to computer vision and its applications, Image formation, Geometric primitives and transformations. IMAGE PROCESSING: Point operators, Linear filtering, More neighborhood operators, Fourier transforms, Pyramids and wavelets, Geometric transformations, Global optimization. FEATURE DETECTION AND MATCHING: Points and patches, Edge Detection methods (Laplacian detectors and Canny edge detector), Harris corner detector, Histogram of Gradients, SIFT, Color and Texture, Feature based alignment, least squares and RANSAC. CAMERA CALIBRATION: Camera models, Stereo vision, Stereo correspondence, Epipolar geometry. TRACKING: Optical flow, Lucas Kanade method, KLT tracking method, Mean shift method, Dense motion estimation. 3D CONSTRUCTION: Shape from X, Surface representations, Point-based representations, Model-based reconstruction, Recovering texture maps. OBJECT RECOGNITION: SVM, Face detection and recognition, Bag of words, Deep learning.

**References:**

1. Richard Szeliski, Computer Vision: Algorithms and Applications, Springer 2011.
2. David A. Forsyth and Jean Ponce, Computer Vision: A Modern Approach, PHI learning 2015.
3. Jan Erik Solem, Programming Computer Vision with Python, O’Reilly, 2012

**<u>Course Outcomes</u>**

After completing the course, the student will be able to:

CO1: Understand the concepts of image formation, colour models and linear filtering.

CO2: Understand the mathematics behind feature detection and description methods.

CO3: Demonstrate a thorough understanding of fundamental concepts in camera calibration.
CO4: Understand and analyze various object tracking algorithms.
CO5: Comprehend object and scene recognition and categorization from images.

## CSE 5254 FUNDAMENTALS OF QUANTUM COMPUTING [4 0 0 4]

Introduction, Fundamental concepts. Quantum bits, Quantum computation, Quantum algorithms, Quantum Information, Introduction to Quantum Mechanics, Liner algebra, Postulates of quantum mechanics, Quantum Computation, Quantum circuits, Controlled operations, Measurement, Universal quantum gates, The Quantum Fourier Transform, The quantum Fourier transform, Phase estimation, Applications, Quantum Search Algorithms, Quantum counting, Speeding up the solution of NP-Complete problems, Quantum Information, Classical noise and Markov processes, Quantum Operations, Quantum Error Correction, The Shor code, Theory of quantum error correction, Entropy and Information, Shannon entropy, Basic properties of entropy, Von Neumann entropy, Quantum Information Theory, Distinguishing quantum states and the accessible information, Data compression, Classical information versus noisy quantum channels, Quantum information versus noisy quantum channels, Entanglement as a physical resource, Quantum cryptography.

**References:**

1. Michael A Nielsen, and Isaac L. Chuang "*Quantum Computation & Quantum Information"*, (10e), Cambridge University Press, 2011.
2. F. Benatti, M. Fannes, R. Floreanini, and D. Petritis, "*Quantum Information, Computation and Cryptography"* Springer, 2010.
3. Mika Hirvensalo, "*Quantum Computing",* (2e), Springer-Verlag New York, 2004.
4. Jozef Gruska, "*Quantum Computing"*, McGraw Hill, 1999.
5. Phillip Kaye, Raymond *Laflamme* and Michele Mosca, "*An Introduction to Quantum Computing*", Oxford University Press, 2006.

**Course Outcomes**

After completing the course, the student will be able to:

CO1: Learn basic concepts in quantum mechanics.
CO2: Understand quantum computation techniques.
CO3: Study and analyse quantum information theory.
CO4: Understand concept of entropy and quantum codes.
CO5: Learn quantum computation algorithms

## CSE 5013 SYSTEM AND NETWORK SECURITY [4 0 0 4]

Introduction: CIA Triad, Defence Models, Computer Viruses: Genesis, Classification. Risk analysis: Threats, types of attacks, worms, trojans, buffer overflow, poisoning, risk analysis. Intrusion detection systems, types, changing nature of IDS tools, challenges, implementation, intrusion prevention systems, intrusion detection tools. Operating system security: OS models, classic security models, reference monitor, international standards for operating system security. Firewalls: Types, implementation, Demilitarized Zone, Firewall forensics, Firewall Services and Limitations. IPSec: IPv4 and Ipv6, SKIP, IKE phases, Session Keys, Message IDs, Phase 2/Quick Mode, Traffic selectors, IPSec SA. PGP: Overview, Key distribution, Efficient encoding, Signature Types, Key rings, Anomalies and Object formats. Kerberos: Version 4, Realms, Interrealm authentication, Message formats. Kerberos V5 ASN.1, KDC Database, Kerberos V5 Messages.

**References:**

1. Mark Rhodes Ousley, "*The Complete* Reference*: Information Security*", (2e), Mc Graw Hill Publication, 2013.
2. Peter Szor, "The art of Computer Virus Research and Defense", Addison Wesley Professional, 2005.
3. Joseph Migga Kizza, "Guide to Computer Security", (3e), Springer,2015.
4. Charlie Kaufman, Radia Perlman, Mike Speciner, "Network Security : PRIVATE Communication in a PUBLIC World", (2e), Pearson Education, 2005.
5. William Stallings, "Cryptography and Network Security Principles and Practice", (6e), Prentice Hall, 2014.

**Course Outcomes**

After completing the course, the student will be able to:

CO1: Identify defence models, security risks and analyse different types of viruses.

CO2: Recognize system intrusion, and apply prevention methods

CO3: Analyse OS security models and write firewall policies.

CO4: Identify different modes of security at the IP layer.

CO5: Apply protocols for authentication and e-mail security.

## CSE 5014 CYBER FORENSICS [4 0 0 4]

Computer Forensic: History, Computer Investigations, Law Enforcements, Storage Format, Digital Evidence, Hash Functions, File Structures, Software Preview, Email Services, Forensic in Networks, Digital Emails, Forensic in Mobiles, High Technology Investigations, Forensic Witness's, Service Virtualization, Rogue Machines, Data Storage, Malware Forensics, Memory Forensics, Post Mortem Forensics, profiling Forensics, Service Virtualization, Virtual Privacy Machines, MS Analysis Tools, Forensic Compliance, Virtual Appliances, Encryption, Decryprtion, Volatile Data Collection, Process Models, Data Protection, File Signatures, Artifacts, Use Cases, report Writing, Expert Investigations, Case Hearing, Testimony, File Formats, Digital Emails, Email Investigations, Mobile Data Investigations.

**References:**

1. Bill Nelson, Amelia Philips, Frank Enfinger, Christofer Steuart, Computer F0rensics and Investigations, Cengage Learning India Private Limited, 2009.
2. Eoghan Casey, Digital evidence and Computer Crime, Edition 3, Academic Press, 2011.
3. Mrjie Britz, Computer Forensics and Cyber Crime, Edition 2, Prentice Hall, 2012.
4. Diane Barrett, Greg Kipper, Virtualization and Forensics, A Digital Forensic Investigator's Guide to Virtual Environments, Elsevier , 2010.
5. Malware Forensics Investigating and Analyzing Malicious Code, James M Aquilina, Eoghan Casey, Cameron H Malin, Elsevier, 2008.

**Course Outcomes**

After completing the course, the student will be able to:

CO1: To build strong foundation in Forensics.

CO2: To understand applications of Cyber Space in Forensics.

CO3: To understand data and files in Cyber Forensics.

CO4: To understand Virtual Forensics and it's link to Cyber Space.

CO5: To understand Malware Forensics and it's applications.

## CSE 5015 BLOCKCHAIN TECHNOLOGY AND APPLICATIONS [4 0 0 4]

Introduction, Structure of a Block, The Genesis Block, Linking Blocks in the Blockchain, Merkle Trees, Simplified Payment Verification, Using hash functions to chain blocks, for Proof-of-Work, Digital Signatures to sign transactions, Distributed Ledger, Byzantine Agreement, Eventual Consistency & Bitcoin Consistency- Availability and Partitions, Bitcoin, Smart Contracts, Weak Consistency, Distributed Storage, Consistent Hashing, Hypercubic Networks, Mining and Consensus: Decentralized Consensus, Independent Verification of Transactions Mining Nodes, Aggregating Transactions into Blocks, Constructing the Block Header, Successfully Mining the Block, Validating a New Block, Assembling and Selecting Chains of Blocks, Consensus Attacks, Changing the Consensus Rules, Soft Fork Signaling with Block Version, Consensus Software Development, Ethereum and Bitcoin, block format, mining algorithm, proof-of-stake (PoS) algorithm, account management, contracts and transactions, Solidity language, account management, contracts and transactions, Applications of Blockchain :Case studies

**References:**

1. Andreas M. Antonopoulos, "Mastering Bitcoin: unlocking digital cryptocurrencies", O'Reilly Media, (1e) 2014

2. Roger Wattenhofer, “Distributed Ledger Technology, The science of the Blockchain”, Inverted Forest Publishing, (2e), 2017.
3. Antonopoulos, Andreas M. and Wood, Gavin. “Mastering Ethereum”, O’Reilly Media, 2018.
4. George Icahn, “Blockchain:the complete guide to understanding blockchain technology”, Amazon publishers, 2017.

**Course Outcomes**

After completing the course, the student will be able to:

CO1: Explain the concept of block in a blockchain and its immutable property

CO2: Appreciate the working of distributed ledger

CO3: Analyze the various consensus protocols

CO4: Use of Ethereum to implement Blockchain

CO5: Identify and apply blockchain approaches for various real world applications

## CSE 5016 CYBER LAW AND ETHICS [4 0 0 4]

Introduction To Cyberethics: Concepts, Perspectives,And Methodological Frameworks. Ethical Concepts And Ethical Theories: Establishing And Justifying A Moral System. Critical Reasoning Skills For Evaluating Disputes In Cyberethics. Professional Ethics, Codes Of Conduct, And Moral Responsibility. Privacy And Cyberspace. Security In Cyberspace. Cybercrime And Cyber-Related Crimes. Intellectual Property Disputes In Cyberspace. Regulating Commerce And Speech In Cyberspace. The Digital Divide, Democracy, And Work. Online Communities, Cyber Identities, And Social Networks. Ethical Aspects Of Emerging And Converging Technologies. Preliminary, Digital Signature, Electronic Governance, Attribution, Acknowledgment And Dispatch Of Electronic Records, Regulation Of Certifying Authorities, Duties Of Subscribers, Penalties And Adjudication, The Cyber Regulations Appellate Tribunal, Offences, Network Service Providers Not To Be Liable In Certain Cases, Miscellaneous. The Patents Act 1970-incorporating all amendments and rules-till 2015. Copy Right Act 1957-incorporating all amendments and rules-till 2015.

**References:**

1. Herman T. Tavani, “*Ethics and Technology Controversies, Questions, and Strategies*” (4e) Wiley, 2013.
2. The Information Technology 2000 (incorporating all amendments and rules-till 2015)-Bare Act
3. The Patents Act 1970(incorporating all amendments and rules-till 2015)-Bare Act
4. Copy Right Act 1957(incorporating all amendments and rules-till 2015)-Bare Act

**Course Outcomes**

After completing the course, the student will be able to:

CO1: Possess Professional and ethical responsibilities based on community values and the law

CO2: Understand laws and regulations related to computer ethics and individual conduct in cyberspace

CO3: Understand the ethical issues associated with confidentiality and privacy as they relate to information technology.

CO4: Apply critical thinking skills to evaluate cyber ethics issues

CO5: Describe legal and public relations implications of security and privacy issues.

## CSE 5017 DATA HIDING [4 0 0 4]

Introduction, Steganography, and Watermarking, Importance of Watermarking and Steganography. Applications of Watermarking and Steganography, Properties of Watermarking and Steganography, Evaluating Watermarking and Steganographic Systems, Mathematical models for Information hiding, Steganographic Techniques, Steganographic Communication, Information-Theoretic Foundations of Steganography, Cachin's Definition of Steganography, Practical Steganographic Methods, Statistics Preserving Steganography, Model-Based Steganography, Minimizing the Embedding Impact, Steganalysis: Detection, Forensic Steganalysis, Some Significant Steganalysis Algorithms, Digital watermarking: Types and Approaches, Models of Watermarking, Informed Embedding, Watermarking using Side Information, Implementing DM with a Simple Lattice Code, Robust watermarking: Approaches, Robustness to Valumetric, Temporal and Geometric Distortions, Watermark Security: Security Requirements, Categories of Attacks.

**References:**

1. Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker, "*Digital Watermarking and Steganography*", (2e), Morgan Kaufmann, 2007
2. WeiQi Yan, Jonathan Weir, "*Fundamentals of Media Security"*, Ventus Publishing ApS, 2010.
3. Stefan Katzenbeisser and Fabien A.P. Petitcolas, "*Information hiding techniques for steganography and digital watermarking*", Artech House Inc, 2000.
4. Michael T. Raggo and Chet Hosmer, "*Data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols*", Syngress, 2012.
5. Husrev Sencar, Mahalingam Ramkumar, Ali Akansu, "*Data Hiding Fundamentals and Applications*", Academic Press, 2004.

**Course Outcomes**

After completing the course, the student will be able to:

CO1: Explain the various techniques for data hiding and analyse models of data hiding
CO2: Choose steganographic techniques for different applications
CO3: Perform steganalysis using various algorithms
CO4: Apply water marking techniques for different domains
CO5: Use the data hiding techniques for digital rights management

## CSE 5018 DATABASE AND APPLICATION SECURITY [4 0 0 4]

Introduction, Database security, Operating systems overview, security environment, Authentication methods, Vulnerabilities of operating systems, Defining and using profiles, Designing and implementing password policies, Granting and revoking user privileges, Obfuscate application code, Secure the database from SQL injection attacks, Beware of double whammies: Combination of SQL injection and buffer overflow vulnerability, Types of users, security models, application types, application security models and Data encryption, Implementing VPD, Implementing oracle VPD, Auditing overview, environment, process, objectives, classification and types, Benefits and side effects of auditing, Map data sources and sinks, Understand Web services security before exposing Web services endpoints, Auditing Database Activities: Introduction, usage of database activities, creating DLL triggers, auditing database activities with oracle, Security and Auditing project cases: Introduction, Case Study for developing an online database.

**References:**

1. Hassan A. Afyouni, *Database Security and Auditing*, India Edition, CENGAGE Learning, 2009.
2. RonBen Natan, *Implementing Database Security and Auditing*, Elsevier, Indian Reprint, 2006.
3. M.TamerÖzsu, Patrick Valdureiz, *Principles of Distributed Database Systems*, Prentice Hall, (2e), Springer, 2011.
4. Castano, Fugini, *Database Security*, Addison Wesley, ACM, 2004.
5. Clark, Holloway, *The Security Audit and Control of Databases*, List, UK, Ashgate, 2011.
6. Douglas, *Security and Audit of Database System*, Blackwell, UK, 2010.
7. Fernandez, Summers, Wood, *Database Security and Integrity*, Addison Wesley, 2012.

**Course Outcomes**

After completing the course, the student will be able to:

CO 1: Explain Security Architecture and Applications.
CO 2: Analyze Authentication and its applications.
CO 3: Explain properties of databases in terms of authentication.
CO 4: Analyze Models for Security Applications.
CO 5: Explain Framework for Security.

## CSE 5019 DISTRIBUTED AND CLOUD SECURITY [4 0 0 4]

User Authentication and Access Control : Electronic User Authentication Principles , Password-Based, Token-Based, Biometric and Remote User Authentication, Access Control Principles , Attribute-Based Access Control ,Identity, Credential, and Access Management ,Trust Frameworks Application Level and service level Vulnerabilities and Attacks, Denial-of-Service Attacks and Intrusion detection, cloud software security, cloud computing risk issues and security challenges, Cloud Computing Risk Issues The CIA Triad Privacy and Compliance Risks Threats to Infrastructure, Data, and Access Control Cloud Service Provider Risks Summary, Cloud Computing Security Challenges Security Policy Implementation Virtualization Security Management Summary.cloud security architecture Issues Standards Incident Response Encryption and Key Management Retirement Summary.

**References:**

1. William Stallings Lawrie Brown “*Computer Security Principles and Practice*” (3e) Pearson-2015.
2. Abhijit Belapurkar, Anirban Chakrabarti, Harigopal Ponnapalli, Niranjan Varadarajan, Srinivas Padmanabhuni, Srikanth Sundarrajan , “*Distributed Systems Security: Issues, Processes and Solutions*”, Wiley 2009.
3. Ronald L. Krutz, Russell Dean Vines “*Cloud Security, A Comprehensive Guide to Secure Cloud Computing*” Wiley; (1e)-2010.
4. Vines Russell Dean, “*Cloud Security*”, Wiley 2015.

**Course Outcomes**

After completing the course, the student will be able to:

CO1: Understand the concepts of authentication and access control

CO2: Understand the concept of Application and service level security.

CO3: Ability to understand denial of service attack detection and prevention.

CO4: Understand the issues of Cloud security architecture and cloud software security.

CO5: Understand the cloud computing risk issues and security challenges.

## CSE 5020 HARDWARE SECURITY [4 0 0 4]

Introduction, Finite Fields. Advanced Encryption Standard (AES) Hardware, S-box. Introduction to Elliptic Curve Cryptography (ECC). The field-programmable gate array ( FPGA) architecture, the FPGA design flow, the mapping of algorithm to hardware. Enhancing the performance of hardware design. Hardware design of AES, efficient design of Finite Field Arithmetic on FPGAs, high speed implementation of Elliptic Curve scalar multiplication on FPGAs. Introduction to Side Channel Analysis (SCA), Power attacks, Fault attacks, Cache attacks, Scan chain based attacks. Differential fault analysis of Ciphers, Cache attacks on ciphers, Power analysis of ciphers implementation, Countermeasures against SCA, Testability of cryptographic hardware. Overview techniques for hardware Trojan detection, Introduction PUFs. Design on FPGAs

**References:**

1. Debdeep Mukhopadhyay and Rajat Subhra Chakraborty, " *Hardware Security: Design, Threats and Safeguards* ", CRC Press, 2015.
2. Mohammad Tehranipoor and Cliff Wang, " *Introduction to Hardware Security and Trust* ", Springer, 2011.
3. Nadia Nedjah and Luiza de Macedo Mourelle, " *Embedded Cryptographic Hardware: Design & Security* , Nova Publishers, 2005.
4. Stefan Mangard and Elisabeth Oswald and Thomas Popp, " *Power Analysis Attacks: the Secrets of Smart Cards* ", Springer, 2007.

**Course Outcomes**

After completing the course, the student will be able to:<br>
CO1: Learning the state-of-the-art cryptographic hardware design techniques
CO2: Protection of the design against privacy and tampering
CO3: Understanding of side channel attacks and providing countermeasures against them
CO4: Understanding secure design of hardware techniques
CO5: Understanding latest mitigation mechanisms against hardware threat

## CSE 5021 INFORMATION SECURITY MANAGEMENT [4 0 0 4]

Introduction To Information Security, Characteristics of Information, NSTISSC Security Model, Components of an Information System, Security Systems Development Life Cycle, Security Professional and The Organization. Security Policies: Access Control Matrix, Confidentiality Polices: The Bell-LaPadula Model, Integrity Policies: Biba Integrity Model, The Clark-Wilson Integrity Model, Hybrid Policies: Chinese Wall Model. Threats, Attacks, An Overview of Risk Management, Risk Identification, Identifying Assets, Threats and Vulnerabilities, Risk Control Strategies, Selection A Risk Control Strategy. Quantitative Versus Qualitative Risk Control Practices, Planning For Security, Introduction To Assurance, Implementing Information Security, Vulnerability Analysis, Penetration Testing, Layering of tests, Vulnerability Classification Auditing, Anatomy of an auditing system, designing an auditing system, Auditing mechanisms, Audit browsing.

**References:**

1. Michael E. Whitman and Herbert J. Mattord, "*Principles of Information Security",* (6e), Thomson Learning, 2018.
2. Matt Bishop, Introduction to Computer Security, Pearson , 2011.

**Course Outcomes**

After completing the course, the student will be able to:

CO1: Understanding security system development process.

CO2: To study various information security policies and attacks.

CO3: Understanding various risk management strategies.

CO4: Learn to build secure and trusted system.

CO5: Understanding vulnerability analysis.

## CSE 5022 INTERNET OF THINGS SECURITY [4 0 0 4]

Overview of Internet of Things (IoT), IoT architectures, applications of IoT, issues and challenges in IoT, future research directions in IoT security, System model for IoT, Evolution of the networks, vision of the Internet of Things- large scale ubiquitous and pervasive connectivity, Vulnerable features of the Internet of Things, threat taxonomy, system security threats, reflective trust and reputation threats, Making the IoT more secure and private, protocol and network security, data and privacy, identity management, trust management, fault tolerance, social awareness, Security protocols in IoT, authentication protocols in IoT, single-server authentication protocols, multi-server authentication protocols, attacks on IoT authentication protocols, informal and formal security proofs for IoT authentication protocols, access control protocols in IoT, privacy preserving data dissemination protocols in IoT, malware propagation and control technique in IoT. Case studies for selected IoT deployments, Internet of Vehicles (IoV), Healthcare of Things, Internet of Drones (IoD). Testbed implementations and simulations of IoT security protocols

**References:**

1. S. Misra, M. Maheswaran, S. Hashmi. “Security Challenges and Approaches in Internet of Things”, (2e), Springer Briefs in Electrical and Computer Engineering, 2017.
2. C. Patel, N. Doshi, “Internet of Things Security: Challenges, Advances, and Analytics”, (1e), CRC press, 2018.
3. F. Hu. “Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations”, (1e), CRC press, 2016.

**Course Outcomes**

After completing the course, the student will be able to:

CO1: Understand the different architectures of Internet of Things.

CO2: Analyse and explain various threats and attacks in Internet of Things communication environment.

CO3: Identify various protocols used for securing Internet of Things communication.

CO4: Design and implement different protocols which can be used for securing Internet of Things communication.

CO5: Perform testbed simulation of Internet of Things communication environment.

## CSE 5023 MOBILE AND WIRELESS SECURITY [4 0 0 4]

Introduction to Security and Privacy for Mobile and Wireless Networks, Pervasive Systems, Trust Negotiation- Extending Trust Negotiation to Support Privacy , Mobile system architectures and Security & Attacks, Wireless security, Attacking 802.11 Networks, Attacking WPA protected 802.11 Networks, Bluetooth Scanning, Bluetooth Eavesdropping, Attacking and Exploiting Bluetooth, Bluetooth Security solutions, ZigBee Security, ZigBee Attacks, Security in Ad Hoc Wireless Networks, Network Security Requirements, Issues and Challenges in Security Provisioning, Network Security Attacks, Key Management in Ad hoc Wireless Networks, Key Management in Wireless Sensor Networks, Secure Routing in Ad hoc Wireless Networks, RFID: an anti-counterfeiting tool, Efficient and Secure RFID Security Method, Optimizing RFID protocols for Low Information Leakage, VoIP, IP Multimedia Subsystem (IMS), 4G security, Confidentiality, Attacks on wireless sensor networks and counter-measures, Prevention mechanisms: authentication and traffic protection.

**References:**

1. Lei Chen, Jiahuang Ji, Zihong Zhang, “Wireless Network Security”, (1e), Springer Science & Business Media, 2013.
2. Johny Cache, Joshua Wright and Vincent Liu, Hacking, “Wireless Exposed: Wireless Security Secrets & Solutions”, (3e), McGraw-Hill Osborne, 2015.
3. Kia Makki, Peter Reiher, “Mobile and Wireless Network Security and Privacy”, (2e), Springer, 2010.
4. Noureddine Boudriga, “Security of Mobile Communications”, (1e), CRC Press, 2009.
5. Kitsos Paris, Zhang Yan, “RFID Security Techniques, Protocols and System-On-Chip Design”, (5e), Springer, 2011.

**Course Outcomes**

After completing the course, the student will be able to:

CO1: Understand wireless fundamentals like wireless network protocols and technologies.

CO2: Analyze and Design security architectures applied in mobile/wireless communications

CO3: Develop secure WLANs.

CO4: Design and Analyze security in GSM, 3G and RFID

CO5: Understand security issues with respect to next generation mobile networks

## CSE 5024 SECURE SOFTWARE DESIGN [4 0 0 4]

Introduction to CIA triads, Fighting fire, The human Factor, The Network, Data-Centric Threats, Business Application, Introducing eve, The Science of Secrecy, Eve Unleashed, Malicious Modifications and Insidious Insertions, Play it Again, Eve in the Middle, Making the Connection, Roll Up the Welcome Mat, The Why in What and How, Business Application, Common Operating Systems, Operating Systems Threats, Operating System Defects Tactics, Auditing and Monitoring, Backup and Redundancy, Remote Access Security, Virtualization, The Logical Design, The physical design, Buffer Bashing, Good Input, Good Output, Inherent Inheritance and Overdoing Overloads, The Threatdown, The Client a Risk, The Biggest Threats to Web Applications, Javascript and AJAX, Adobe Flash, ActiveX, Simplify, Restrict and Scrub, Prediction Through Penetration Testing, The Insider Threat and Beyond, Migration to Defend Against the Unknown, The Organization Incidence Response, The Business Continuity Plan, Becoming and Staying Proactive

**References:**

1. Theodor Richardson, "*Secure Software Design*", (3e), Jones & Barlett Learning, MIT Press, 2013.
2. Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hyberstson, Frank Bushcmann, and Peter Sommerlad, *"Security Patterns Integrating Systems Engineering"*, Wiley Series in Software Design Patters, 2006
3. John Viega, Gary R. McGraw, *"Building Secure Software: How to Avoid Security Problems the Right Way, Portable Documents"*, Pearson Education, 2006
4. Gary McGraw, "Software Security: Building Security in", Addison-Wesley Professional, 2006

**Course Outcomes**

After completing the course, the student will be able to:

CO1: To understand the likely point of attacks, pre deciding how the software will deal with the attacks

CO2: To analyze the security requirement, design, implementing, verification and deployment in real time environment

CO3: To construct software that can deal with both known and unknown attacks

CO4: To understand the business application need for secured software

CO5: To identify the real time web application threats and risk mitigation

# OPEN ELECTIVES

## CSE 5051 DEEP LEARNING [3 0 0 3]

Introduction to neural networks: Humans Versus Computers, Basic Architecture, Training, Practical Issues, Common Neural Architectures, Advanced Topics. Machine learning with shallow neural networks: Binary and Multiclass Models, Autoencoders. Fundamentals of deep networks: What is Deep Learning, Architectural Principles, Building blocks. Training deep neural networks. Gradient-Descent Strategies, Batch Normalization, Acceleration and Compression. Recurrent neural networks (RNN): Architecture, Challenges, Echo State Networks, Long Short Term Memory, Gated Recurrent Units, Applications of RNN. Convolutional neural networks (CNN): Basic Structure, Training a CNN, Case studies of Convolutional Architectures, Visualization and Unsupervised Learning; Autoencoders. Applications of CNN. Advanced topics in deep learning: Attention mechanisms, Generative Adversarial Networks, Competitive Learning.

**References:**

1. Charu C Aggarwal, "*Neural Networks and Deep Learning*", Springer International Publishing, 2018.
2. Josh Patterson and Adam Gibson, "*Deep Learning: A Practitioner's Approach*", Oreilly, 2018.
3. Ian Goodfellow, Yoshua Bengio, Aaron Courville, "*Deep Learning*", MIT Press, 2016.
4. Relevant research papers.

### Course Outcomes

After completing the course, the student will be able to:

CO1: Understand different neural network architectures.

CO2: Identify architectural principles of shallow and deep neural networks.

CO3: Analyse the training parameters of deep networks and train RNN.

CO4: Analyse convolutional architectures and their applications.

CO5: Understand advanced topics in deep learning.

## CSE 5052 SOFTWARE PROJECT MANAGEMENT AND QUALITY ASSURANCE [3 0 0 3]

Importance of Software Project Management, Management Principles, Strategic Program Management, Stepwise Project Planning. Project Schedules, Critical Path (CRM) Method, Risk Identification, Cost Schedules. Framework for Management and Control, Collection of Data Project Termination, Managing People, Organizational Behavior, Decision Making, Team Structures, Communication Plans, Case study. Need for Software Quality, Software Quality Assurance, Software Quality factors, Software Development methods, Quality Assurance Activities, Software Maintenance Quality, and Project Management. Staff Training and Certification Corrective and Preventive Actions, Project Process Control, Computerized Tools, Software Quality Metrics, Limitations of Software Metrics, Cost of Software Quality, Classical Quality Cost Model, Extended Model, Application of Cost Model.

**References:**

1. Bob Hughes, Mike Cotterell and Rajib Mall, "*Software Project Management*" (5e), Tata McGraw Hill, New Delhi, 2012.
2. Robert K. Wysocki, *"Effective Software Project Management"* (4e) – Wiley Publication, 2011.
3. Gopalaswamy Ramesh, *"Managing Global Software Projects"* – McGraw Hill Education (India), Fourteenth Reprint 2013.
4. Rajib Mall, "Fundamentals of Software Engineering" PHI Learning PVT. LTD, 4th Edition, 2014
5. Marcelo Marinho et.al; "A Systematic review of Uncertainties in Software Project Management", International Journal of Software Engineering & Applications (IJSEA), Vol.5, No.6, November 2014.
6. Daniel Galin, *"Software Quality Assurance"*, ISBN 0201 70945 7, Pearson Publication, 2009.
7. Alan C. Gillies, *"Software Quality: Theory and Management"*, International Thomson Computer Press, 1997.

**Course Outcomes:**

After completing the course, the student will be able to:

CO1: Understand the basic tenets of Software Quality and its factors and be exposed to Software Quality Assurance (SQA) with its components.

CO2: Understand how the SQA components be integrated into the Software Project life cycle.

CO3: Be familiar with the Software Quality Infrastructure and staffing principles.

CO4: Utilize the concepts in Software Development Life Cycle and demonstrate their capability to adopt high quality standards.

CO5: Assess the quality of software product.