UTKAL UNIVERSITY

Syllabus

for

Master of Technology in

Computer Science (M. Tech (CS))

(2-Years Programme)

Department of Computer Science & Applications
Utkal University
Bhubaneswar (Odisha)

2021-22

UTKAL UNIVERSITY

Syllabus for Masters of Technology in Computer Science (M. Tech (CS))

(Applicable for Students Taking Admission from the Session 2021-22)

Objective of the Course

The objective of the M. Tech curriculum is to equip the students with the ability to analyze varieties of real-life problems and develop research based solutions. Keeping in view the research and development requirements of the evolving software industry and also to provide a foundation for higher studies in Computer Science, effort has been made in the choice of subjects to balance between theory and practical aspects of Computer Science. On successful completion of this course a student can find a career in the Academics or R&D wing of Corporate Sectors, or Government Organizations as a technical professional or pursue research in the core areas of Computer Science.

Eligibility Criteria

The candidate should have passed (a) Master of Computer Applications (MCA) (b) Master's Degree in Computer Science / IT/ Mathematics / Statistics / Electronics / Physics or (c) Bachelor's Degree in Engineering / Technology (BE / B. Tech / AMIE in CSE/ IT/ ECE/ EE/ EEE/ EIE) / Grad IETE or (d) B level examination of NIELIT with at least 55% of marks (50% marks for SC/ST candidates) in the qualifying examination.

Syllabus for Masters of Technology in Computer Science(M. Tech (CS))				
PAPER ID	**PAPER TITLE**	**FULL MARK**		**CREDIT**
		Mid-Term	**End-Term**	
FIRST SEMESTER				
MT-1.1	Discrete Mathematics	30	70	4
MT-1.2	Data Structure & Algorithm Design	30	70	4
MT-1.3	Advanced Computer Architecture	30	70	4
MT-1.4	Advanced Computer Network	30	70	4
MT-1.5	Elective-I	30	70	4
MT-1.6	Elective-II	30	70	4
MT-1.7	Unix & C Programming Lab		50	2
MT-1.8	Data Structure & Algorithm Lab		50	2
MT-1.9	Computer Network Lab		50	2
SECOND SEMESTER				
MT-2.1	Theory of Computation	30	70	4
MT-2.2	Advanced Operating System	30	70	4
MT-2.3	Database Engineering	30	70	4
MT-2.4	Advanced Software Engineering	30	70	4
MT-2.5	Elective-III	30	70	4
MT-2.6	Elective-IV	30	70	4

MT-2.7	Operating System Lab		50	2
MT-2.8	Database Lab		50	2
MT-2.9	Software Engineering Lab		50	2
THIRD SEMESTER				
MT-3.1	Machine Learning	30	70	4
MT-3.2	Parallel & Distributed Computing	30	70	4
MT-3.3	Research Methodology	30	70	4
MT-3.4	Cryptography & Network Security	30	70	4
MT-3.5	Elective-V	30	70	4
MT-3.6	Elective-VI	30	70	4
MT-3.7	Machine Learning Lab		50	2
MT-3.8	Network Security Lab		50	2
MT-3.9	Seminar & Technical Writing		50	2
FOURTH SEMESTER				
MT-4.1	Comprehensive Viva	50		2
MT-4.2	Dissertation	300*		12
	Total	**2600**		**104**

List of Elective Papers #

Elective-I	
MT-1.5(1)	Computer Graphics & Multimedia
MT-1.5(2)	Mathematics for Data Science
MT-1.5(3)	Digital Signal Processing
MT-1.5(4)	Combinatorics & Graph Theory
MT-1.5(5)	Soft Computing
Elective-II	
MT-1.6(1)	Probability & Statistics
MT-1.6(2)	Simulation & Modeling
MT-1.6(3)	Network Programming
MT-1.6(4)	Cyber Security
MT-1.6(5)	Bio Informatics
Elective-III	
MT-2.5(1)	Wireless Sensor Networks
MT-2.5(2)	Information Theory & Coding
MT-2.5(3)	Computational Geometry
MT-2.5(4)	Stochastic Modeling & Analysis
MT-2.5(5)	Quantum Computing
Elective-IV	
MT-2.6(1)	Data Warehousing & Mining
MT-2.6(2)	Mobile Computing
MT-2.6(3)	Cloud Computing
MT-2.6(4)	Digital Image Processing
MT-2.6(5)	Social Network Analysis
Elective-V	
MT-3.5(1)	Internet of Things
MT-3.5(2)	Distributed Database System

MT-3.5(3)	VLSI Design
MT-3.5(4)	Computational Complexity
MT-3.5(5)	Software Defined Networks
Elective-VI	
MT-3.6(1)	Big Data Analytics
MT-3.6(2)	Human Computer Interaction
MT-3.6(3)	Block Chain Technology
MT-3.6(4)	Speech & Natural Language Processing
MT-3.6(5)	Intrusion Detection Systems

* **Mark Distribution for Dissertation:**
Report (200), Presentation (50), Viva Voce (50)

 # A student can opt for only one paper from among the papers mentioned under the respective elective groups

N.B. Students may opt at most two elective papers from SWAYAM/NPTEL courses during the programme.

MT-1.1: DISCRETE MATHEMATICS

Objective:

The course objective is to provide students with an overview of discrete mathematics. Students will learn about topics such as logic and proofs, propositional Logic, predicate logic, algebraic structure, graph theory, matrices and other important discrete math concepts.

Learning Outcomes:

At the end of this course student will be able to:

- Express a logic sentence in terms of predicates, quantifiers, and logical connectives.
- Apply the rules of inference and methods of proof including direct and indirect proof forms, proof by contradiction, and mathematical induction**.**
- Use tree and graph algorithms to solve problems.

UNIT-I

Propositional Logic: Declarative sentences, Natural reductions, Propositional Logic and a formal language, Normal forms

UNIT-II

Predicate Logic: The needs for a richer language, Predicate logic as formal language, Proof Theory of predicate logic, Semantics of predicate logic Relations, Equivalence Relations, Functions, Boolean Algebras.

UNIT-III

Algebraic Structure: Monoids and Groups, Binary Group Codes, Lattices, Rings, Integral Domains, Fields, Fields, Ideals, Polynomial Rings, Polynomial Codes.

UNIT-IV

Graph Theory (I): Definition of Graph, The Degree of Vertex, Sub Graphs, Degree sequences, Connected Graphs, Cut-Vertices and Bridges,Special Graphs, Digraphs, Properties of Trees, Depth First Search & Breadth First Search.

UNIT-V

Graph Theory (II): Eulerian Graphs and their characterization, Hamiltonian Graph, Properties of planner Graphs, Vertex Colouring and Chromatic Polynomial.

Text Books:

1. M. R. A. Hulth, M. D. Ryan, Logic in Computer Science: Modeling and Reasoning about systems, Cambridge University Press, 2000, Chapter 1, 2.
2. G. Birkhoff & T. C. Bartee, Modern Applied Algebra, CBS Publishers, 1987. Chapter 1 (1.1 – 1.5), 2 (2.1 -2.6), 5 (5.1 – 5.5, 5.7 – 5.9), 7, 8, 9 (9.1 – 9.4), 10 (10.1, 10.2, 10.5, 10.7), 11 (11.1 – 11.4)
3. K. S. Trivedi, Probability and Statistics with Reliability, Queuing and Computer Science Application – Prentice Hall of India, 2000 (Relevant portion of Ch 1 - 5)
4. G. Chartand & B. R. Oller Mann, Applied and Algorithmic Graph Theory, McGraw Hill 1993, Ch. 1 (1.1 – 1.7), 3 (3.1 – 3.4), 7 (7.1 – 7.2), 8 (8.1 – 8.2), 9 (9.1), 10 (10.1 – 10.2)

MT-1.2: DATA STRUCTURE AND ALGORITHM DESIGN

Objective

The course is designed to develop skills to design and analyze simple linear and nonlinear data structures. It strengthen the ability to the students to identify and apply the suitable data structure for the given real world problem. It enables them to gain knowledge in practical applications of data structures.

Learning Outcomes:

At the end of this course student will be able to:

- Be able to design and analyze the time and space efficiency of the data structure·
- Be capable to identity the appropriate data structure for given problem·
- Have practical knowledge on the applications of data structures.

UNIT-I

Design and Analysis Technique (I): Introduction, Growth of Function, Recurrences, Divide and Conquer (Heap Sort, Quick Sort, Fast Fourier Transforms), Lower bounds of sorting, Counting sort.

UNIT-II

Design and Analysis Technique (II): (Randomized Quick Sort, Primality Testing), Dynamic Programming (Floyd – Warshall Algorithm, Longest Common Subsequence), Greedy Method, (Single Source Shortest Path, Matroids, Task Scheduling).

UNIT-III

Analysis of Data Structure: Binomial Heap, Fibonacci Heaps, Disjoint Sets, Suffix tree, String Matching Algorithm (Ukonnen's algorithm) and applications, Amortised Analysis

UNIT-IV

Maximum Flow: Flow NEWORKS, Ford – Fulkerson Method, Maximum Bipartite Matching.
Computational Geometry: Line segment Intersection, Convex Hull, Vornoi diagram

UNIT-V

NP-Completeness: Polynomial Time, Polynomial – time verification, NP – completeness and Reliability, NP – Completeness Proofs, NP – Complete Problems.
Approximation Algorithms: The Vertex – Cover Problem, The Travelling salesperson Problem

Text Books:

1. T. H. Coreman, C. E. Leiserson, R. L. Rivest, & C. Steanin – Introduction to Algorithms, Prentice Hall of India, 2003.
2. M. R. Garey & D. S. Johnson, Computers and Interactability – a theory of NP Completeness, W. H. Freeman, 1979.
3. M. De Berg, M. Vankreveld, M. Overmars, O. Schwrzkopf Computational Geometry – spring Verlog 2000.

MT-1.3: ADVANCED COMPUTER ARCHITECTURE

Objective:

The aim of this module is to emphasize on the concept of a complete system consisting of asynchronous interactions between concurrently executing hardware components and device driver software in order to illustrate the behavior of a computer system as a whole.

Learning Outcomes:

At the end of this course student will be able to:

- Understand the Concept of Parallel Processing and its applications
- Implement the Hardware for Arithmetic Operations
- Analyze the performance of different scalar Computers
- Develop the Pipelining Concept for a given set of Instructions
- Distinguish the performance of pipelining and non-pipelining environment in a processor

UNIT-I

Fundamentals of Computer Design: Introduction, The Task of a Computer designer, Technology and usage trends, Cost, Performance measures. Quantitative principles of computer design, /the concept of memory hierarchy.

Instruction set Principles of Examples: Introduction, Classification of Instruction Set Architectures, Memory Addressing, Operations in the Instruction Set, The DLX Architecture, Examples, Power PC and Intel 8086

UNIT-II

Pipelining: Basic concepts, Pipeline for DLX, Pipeline Hazards, Data and Control Hazards, Difficulties in implementation, Instruction Set Design and pipelining. The MIPS R 4000 Pipeline.

UNIT-III

Instruction – Level Parallelism (ILP): Concepts and challenges, Overcoming Data Hazards with Dynamic Scheduling, Reducing Branch Penalties with Dynamic Hazards Prediction, ILP with multiple issue, Hardware Support for Extracting more parallelism, Studies of ILP, The power PC 620.

UNIT-IV

Memory–Hierarch Design : Basic concepts of memory, Internal Organisation of Memory chips, Caches, Reducing Cache Misses and Miss Penalty, Reduction Hit Time, Main Memory, Virtual memory, Issues in the design of Memory Hierarchies, fallacies and Pitfalls in Memory – Hierarchy Design.

Storage System: Types of storage devices, Busses, I/O Performance Measures, Reliability, Availability and RAID, Interfacing to OS, Designing and I/O System, Unix File System Performance.

UNIT-V

Multiprocessor : Taxonomy of Parallel Architecture, Performance Matrices and Advantages for communications Mechanisms, Challenges of Parallel Processing, Characteristics of Application Domains, Centralized Shared memory architectures, Distributed shared – memory architectures, synchronization, Models of memory, Consistency, Performance measurement of

Parallel machines, Memory system Issues, Design and performance of SGI challenges Multiprocessor.

Text Books:

1. J. L. Hennesy & D. A. Patterson – Computer Architecture – A Quantitative Approach, 2nd Edition – Morgan Kaufmann Publishers,1996 [chapters 1, 2, 3, 4, 5, 6, 7, 8]
2. V. C. Hammacher, Z. G. Vranesic, S. G. Zaky – Computer Organisation, McGraw Hill, 1996 [chpters 1, 2, 3, 4, 5, Appendix A].
3. M. M. Mano – Computer System Architecture, 3rd Edition, PHI, 1993.
4. K. Hwang – Advanced Computer Architecture, McGraw Hill, 1993.
5. D. Sima, T. Fountain, P. Kacsak – Advanced Computer Architecture – A Design Space Approach, Addison Wesley, 1997.
6. D. A. Pattereson & J. L. Hennessy – Computer Organisation & Design, Morgan Kaufmann, 1998.

MT-1.4: ADVANCED COMPUTER NETWORKS

Objective:

This course aims to provide advanced background on relevant computer networking topics to have a comprehensive and deep knowledge in computer networks.

Learning Outcome:

At the end of this course student will be able to:

- Recognize the technological trends of Computer Networking.
- Discuss the key technological components of the Network.
- Evaluate the challenges in building networks and solutions to those.

UNIT-I

Direct Link Network: Framing , Error Detection and correction Reliable Transmission Ethernet (802.3, 802.4 FDDI), Wireless (802.11) Network adapter, MAC Layer, Switching & Forwarding, Bridges and LAN switches, cell switching protocols in Data Link Layer.

UNIT-II

Packet Switching and Internetworking: Routing simple Internetworking (I/P), Addressing Subneting global Internet, Multicast, Broadcast, Multiprotocol (BGP, OSPF etc), Mobile IP, Congestion Control Algorithms.

UNIT-III

Transport Layer Congestion Control: TCP, UDP, RPC, Congestion Control and Resource Allocation

UNIT-IV

Application Layer and Network Security: Name Services (DNS), Electronic mails (SMTP, MIME, IMAP), HTTP, SNMP, Multimedia Applications (RTDSIPH323) Cryptogrphy algorithms, Security mechanism, Pretty Good Privacy (PGP), SSH (Secure Shell), Transport Layer Security, Firewall

UNIT-V

Performance Issues/Network Analysis: Stream Session: Deterministic Network Analysis, Stochastic Analysis, Adaptive Bandwidth sharing for Elastic traffic, Multiple Access: Wireless Networks.

Text Books:

1. Peterson L. and Davie S. B. – Computer Networks A System Approach, Kaufman Publishers, 4th edition
2. S. Tanenbaum – Computer Network – PHI, 4th edition
3. Anurag Kumar, D. Manjunath, Joy Kuri – Communication Networking (An Analytical Approach), Morgan Kaufmann publishers, An imprint of Elsevier, 2005.
4. M. J. Donaho, K. L. Calvent – Pocket Guide to TCP / IP Socket Harcourt Indian 2001.

MT-2.1: THEORY OF COMPUTATION

Objectives:

To introduce students to the mathematical foundations of computation including automata theory; the theory of formal languages and grammars; the notions of algorithm, decidability, complexity, and computability.

Learning Outcomes:

At the end of the course students will be able to:

- Use basic concepts of formal languages of finite automata techniques
- Design Finite Automata's for different Regular Expressions and Languages
- Construct context free grammar for various languages
- Solve various problems of applying normal form techniques, push down automata and Turing Machines

UNIT-I

Regular Language and Finite Automata: Deterministic and Non-Deterministic Finite Automata, Equivalent Automata, Minimization of Finite Automata, Regular Languages and Regular Expressions, Closure Properties for Regular Languages, Kliene's Theorem, The Pumping Lemma & its applications. The Myhill – Nerude Theorem

UNIT-II

Context Free Languages & Pushdown Automata: Context Free Grammars and their Derivations Trees, Regular Grammars, Chomsky Normal Form, Bara Hillels Pumping Lemma, Closure Properties for Context – Free Languages, Decision Problems involving CFL, Pushdown Automata, Compilers and Formal Languages.

UNIT-III

The Church – Turing Thesis: Turing Machines, Multiple Turing Machines, Non – Deterministic Turing machines, Enumerators, Definition of Algorithm, Terminology for Describing Turing Machines. Decidability : Decidable Problems concerning regular and Context – Free Languages, The Halting Problem, Turing – Unrecognizable Language.

UNIT-IV

Undecidable Problems from Language Theory, Reduction via Computation Histories, Post Correspondence Problem, Mapping Reducibility, Computable Function. The Recursion Theorem and Applications, Decidability of Logical Theories, Turing Reducibility, Definition of Information.

UNIT-V

Complexity Theory: Review of NP – Completeness, Space Complexity (Savitchi Theorem, The Class PSPACE, The classes L and NL, NL – Completeness) Intractability (Hierarchy Theorems, Relativization, Circuit Complexity), Probabilistic Algorithm (Class BPP), Alternation, Interactive Proof System (1P - PSPACE).

Text Books:

1. J. E. Hopcroft, J. D. Ullman – Introduction to Automata Theory, Languages & Computations – Narosa, 1979.
2. M. Spiser – Introduction to Theory of Computation – PWS Pudblisgers, 1997.
3. M. D. Davis, R. Sigaal, E. J. Weyuker – Computability, Complexity & Languages, Academic Press 1994

MT-2.2: ADVANCED OPERATING SYSTEM

Objective:

The aim of this module is to study, learn, and understand the main concepts of advanced operating systems (parallel processing systems, distributed systems, real time systems, network operating systems, and open source operating systems); Hardware and software features that support these systems.

Learning Outcome:

At the end of this course student will be able to:

- Outline the potential benefits of distributed systems
- Summarize the major security issues associated with distributed systems along with the range of techniques available for increasing system security
- Apply standard design principles in the construction of these systems
- Select appropriate approaches for building a range of distributed systems, including some that employ middleware

UNIT-I

Single Machine Operating System (I): Process, CPU Scheduling (Basic concepts, scheduling criteria and algorithms, algorithm evaluation), Process Synchronization (Critical section problem, Semaphores, Classical Problems of Synchronisation, Critical Regions, Monitors). Deadlocks (Modeling and characterization, Prevention, Avoidance, Detection, Recovery).

UNIT-II

Single Machine Operating System (II): Memory Management, (Address Space, Swapping, Contiguous allocation, paging, segmentation), Virtual Memory (Demand paging, page replacement algorithm, allocation of frames, thrashing, demand segmentation), File System Interface (Access methods, directory structure, protection and consistency), File system Implementation, I/O Systems, Secondary storage structure.

UNIT-III

Distributed Operating Systems: Theoretical Foundations (Limitation of a distributed system, clocks, causal ordering of messages, global state, cuts of a distributed computation, termination detection), Distributed Mutual Exclusion (non-token-based algorithms-Lamport, Ricart-Agrawala and Mackawa's algorithms, token-based algorithms- Suzuki-Kasami, Singhal and Raymond's algorithms), Distributed Deadlock (Basic concepts, deadlock handling strageties, control organization for distributed deadlock detection, distributed deadlock detection algorithms), Classification of Agreement Problems, Solution to Byzantine agreement Problem and application to fault tolerance.

UNIT-IV

Distributed Resource Management & Failure Recovery: Distributed File Systmes (mechanism for building distributed file systems, design issues, case studies, disk space management), Distributed Shared Memory (Central – server, migration, read-replication & full-replication algorithms, memory coherence, coherence, coherence protocols, design issues), Distributed Scheduling (Issues in load distributing algorithms – senders initiated, receiver initiated, systematically initiated & adaptive algorithms, performance comparison, load sharing, policies,

task migration). Recovery (Backward and forward error recovery, recovery in concurrent systems, checkpoints, synchronous and asynchronous check pointing and recovery)

UNIT-V

Case Study of Linux: Kernet (System calls, memory management, paging, inter-process communication, File system, device drivers, multiprocessing, modules and debugging). System Administration (cron, inxinctd, config files etc.), Network Administration (NFS, NIS, AutoFS, Samba).

Text Books:

1. A. Silberschaz and P. B. Galvin – Operating System Concepts 8th Edition, Addison Wesley, 1998.
2. N. Singhal and N. G. Sivaratri – Advanced Concepts in Operating Systems, McGraw Hill, 1994 (Ch. 2 - 14)
3. M. Beck, H. Bome, et.al. – Linux Kernel Programming, 3rd Edition, Pearson Education, 2003.
4. A. S. Tanenbaum – Distributed Operating System, Pearson Education, 2001.
5. G. Colouris, J. Dollimore, I. Kindberg – Distriuted Systems, Concepts and Design, 2nd Edition, Addison Wesley, 2000.

MT-2.3: DATABASE ENGINEERING

Objective:

- To explain basic database concepts, applications, data models, schemas and instances.
- To demonstrate the use of constraints and relational algebra operations.
- Describe the basics of SQL and construct queries using SQL.
- To emphasize the importance of normalization in databases.
- To facilitate students in Database design
- To familiarize issues of concurrency control and transaction management.

Learning Outcome:

At the end of the course the students are able to:

- Apply the basic concepts of Database Systems and Applications.
- Use the basics of SQL and construct queries using SQL in database creation and interaction.
- Design a commercial relational database system (Oracle, MySQL) by writing SQL using the system.
- Analyze and Select storage and recovery techniques of database system

UNIT-I

Relational data model, Integrity constraints, relational Queries, Relational Algebra, Tuple Relational Calculus, Domain Relational Calculus, SQL

UNIT-II

Design Guidelines for relational schemas and its algorithms, Functional dependencies, Reasoning about Functional dependencies, Normal forms (1NF, 2NF, BCNF, 4NF and 5NF), Other kinds of dep3ndencies, Design of Relational Database

UNIT-III

Query Processing and Query Evaluation, External sorting, Evaluating relational operators, Selection Operation, Projection Operation, Join Operation, typical relational Query Optimiser. Translating SQL query into relational algebra, Estimating the cost of a plan, Relational algebra equivalence.

UNIT-IV

Transaction processing, Transaction and system concepts, Schedules and recoverability, Locking techniques and concurrency control, Concurrency control based on timestamp ordering, Multiversion concurrency control techniques, Multiple granularity locking, recovery technique based on Deferred and Immediate update, Database Security, Discretionary Access control.

UNIT-V

Introduction to Distributed Databases, Distributed DBMS Architecture, Storing Data in Distributed DBMS, Distributed Database Design, Semantic Data Control, Distributed Query Processing and Optimization

Text Books:

1. Ramez Elmasri and Shamkant B. Navathe – Fundamentals of Database Systems, Addison Wisely.
2. Raghu Ramakrishnan and Johannes Cehrke, -- Database Management System, McGraw hill.
3. M. T. Ozsu, P. Valdruriez – Principles of Distibuted Database Systems, Pearson Education

MT-2.4: ADVANCED SOFTWARE ENGINEERING

Objective:

To provide an advanced understanding and knowledge of the software engineering techniques, techniques to collect software requirements from client and CASE tools and to understand the importance of these case tools in software development.

Learning Outcome:

At the end of this course student will be able to:

- Analyze the software life cycle models.
- Identify the importance of the software development process.
- Analyze the importance of CASE tools.
- Design and develop correct and robust software products using advanced software engineering techniques.
- Able to understand business requirements pertaining to software development.

UNIT-I

Introduction, Software life cycle modules, Requirements Analysis & Specification, Software design, Function oriented Software Design.

UNIT-II

Introduction to object oriented Analysis and Design, Iterative Development and the unified process, Case Study – The next-Gen POS, Inception, Understanding Requirements, Use case Model, Identifying other requirements, From inception to elaboration

UNIT-III

Elaboration, Use Case Model, Drawing system sequence diagrams, Visualizing concepts, Adding Associations, Adding Attributes, Adding details with operation contracts, Interaction diagrams notation, GRASP, Use case realization, Determining visibility, creating design class diagram.

UNIT-IV

Elaboration Iteration 2: Iteration 2 and other requirements, GOF Design pattern, Special topics on drawing & tools, Planning and Project queues comments on iterative development and the UP Rational Unified Process.

UNIT-V

Coding and Testing, Software reliability & Quality Management, Computer Aided Software Engineering, Software Maintenance.

Text Books:

1. Rajib Mall – Fundamentals of Software Engineering, 2nd Edition, PHI
2. I. Sommerville – Software Engineering, Pearson Education
3. Craig Larman – Applying UML and Patterns – An Introduction to OOA&D and the Unified process, 2nd Edition, Pearson Education Asia.
4. Martin Flower – UML Distilled, Pearson Education
5. G. Booch, I. Jacobson, J. Ramburg – UML User Guide, Pearson Education

MT-3.1: MACHINE LEARNING

Objective:

- To introduce students to the basic concepts and techniques of Machine Learning.
- To develop skills of using recent machine learning software for solving practical problems.
- To gain experience of doing independent study and research.

Learning Outcome:

At the end of this course student will be able to:

- Have a good understanding of the fundamental issues and challenges of machine learning: data, model selection, model complexity, etc.
- Have an understanding of the strengths and weaknesses of many popular machine learning approaches.
- Appreciate the underlying mathematical relationships within and across Machine Learning algorithms and the paradigms of supervised and un-supervised learning.
- Be able to design and implement various machine learning algorithms in a range of real-world applications.

UNIT-I

Linear Methods for Regression and Classification: Overview of supervised learning, Linear regression models and least squares, Multiple regression, Subset selection , Ridge regression, least angle regression and Lasso , Linear Discriminant Analysis , Logistic regression , Naïve Bayes Classifier. K-nearest neighbor.

UNIT-II

Model Assesment and Selection :Bias, Variance, and model complexity, Bias-variance trade off, Optimisim of the training error rate, Esimate of In-sample prediction error, Effective number of parameters, Bayesian approach and B. IC, Cross-validation ,Boot strap methods, conditional or expected test error. Dimensionality reduction (PCA, Kernel PCA, Independent Component analysis, LLE, non-negative matrix factorization, SVD), feature Selection.

UNIT-III

Additive Models, Trees, and Boosting: Generalized additive models, Regression and classification trees , Boosting methods-exponential loss and AdaBoost, Numerical Optimization via gradient boosting , Examples (Spam data, California housing , New Zealand fish, Demographic data)

UNIT-IV

Support Vector Machines (SVM) and Neural network: SVM for classification, Reproducing Kernels, SVM for regression. Model of a neuron, Perceptron learning, Backpropagation, Methods to improve backpropagation, Introduction to deep learning.

UNIT-V

Unsupervised Learning and Random forests: Cluster analysis (k-means, Hierarchical clustering, DBSCAN, spectral clustering), Gaussian mixtures and EM algorithm, Random forests and analysis.

Text Books:

1. Trevor Hastie, Robert Tibshirani, Jerome Friedman *, The Elements of Statistical Learning-Data Mining, Inference, and Prediction*, Second Edition , Springer Verlag, 2009.
2. G. James, D.Witten, T.Hastie, R.Tibshirani - *An introduction to statistical learning with applications in R*, Springer, 2013.G. Booch, I. Jacobson, J. Ramburg – UML User Guide, Pearson Education
3. C. M. Bishop –Pattern Recognition and Machine Learning, Springer, 2006
4. L. Wasserman-All of statistics

MT-3.2: PARALLEL & DISTRIBUTED COMPUTING

Objective:

- Learn about parallel and distributed computers.
- Write portable programs for parallel or distributed architectures using Message-Passing Interface (MPI) library
- Analytical modeling and performance of parallel programs.
- Analyze complex problems with shared memory programming with OpenMP

Learning Outcome:

At the end of this course student will be able to:

- Develop and apply knowledge of parallel and distributed computing techniques and methodologies.
- Apply design, development, and performance analysis of parallel and distributed applications.
- Use the application of fundamental Computer Science methods and algorithms in the development of parallel applications.
- Explain the design, testing, and performance analysis of a software system, and to be able to communicate that design to others.

UNIT-I

The need, scope and issues in Parallel Computing, The PRAM Model of Computation, Performance metrics, Amdhal's Law, Work – Time Formalism and Brent's Theorem, Basic PRAM Algorithm Design Techniques (Pointer Jumping, Divide and Conquer, Algorithm cascading)

UNIT-II

Further PRAM Algorithm design techniques (Partitioning, Euler tour, Symmetry breaking), Lower bounds for PRAM Algorithms, P- Completeness.

UNIT-III

Parallel Programming Platforms: (Control Structures & Communication Model, Physical Organisation, Communication Cost, Routing mechanism),
Communication Operations: (One-to-all and all-to-all broadcast and reduction, Personalized Communication, Scatter & Gather, Speed improvement), Programming using Message Passing Paradigm.

UNIT-IV

Principles of Parallel Algorithms design on distributed memory model: (Decomposition, Tasks and Interactions, Mapping), Methods for containing Interaction overheads, Parallel Algorithm model, Scalability of Parallel Systems, Application to Parallel Sorting and combinatorial search algorithms.

UNIT-V

Parallel Numerical Algorithms for Distributed Systems: Matrix Vector & Matrix – Matrix Multiplication, Solution of Linear Systems (Iterative and Direct Methods. The conjugate gradient method), Fast Fourier Transform

Text Books:

1. J. J'aj'a – An Introduction to Parallel Algorithms, Addison Wesley, 1992

2. V. Kumar, A. Gramma, A. Gupta, and G. Karypis – Introduction to Parallel Computing Design and Analysis of Algorithm – 2nd Edition, Pearson Education, 2003
3. P. Pacheco – Parallel Programming with MPI, Morgan Kaufman, 1997.
4. M. J. Quin – Parallel Programming in C with MPI & OpenMP, TMH, 2003.

MT-3.3: RESEARCH METHODOLOGY

Objective:

- To familiarize participants with basic of research and the research process.
- To enable the participants in conducting research work and formulating research synopsis and report.
- To familiarize participants with Statistical packages such as SPSS/EXCEL.
- To impart knowledge for enabling students to develop data analytics skills and meaningful interpretation to the data sets so as to solve the business/Research problem.

Learning Outcome:

At the end of this course student will be able to:

- Develop understanding on various kinds of research, objectives of doing research, research process, research designs and sampling.
- Have basic knowledge on qualitative research techniques
- Have adequate knowledge on measurement & scaling techniques as well as the quantitative data analysis
- Have basic awareness of data analysis-and hypothesis testing procedures

UNIT-I

RESEARCH FORMULATION AND DESIGN: Motivation and objectives – Research methods vs. Methodology. Types of research, concept of applied and basic research process, criteria of good research. Defining and formulating the research problem, selecting the problem, necessity of defining the problem, importance of literature review in defining a problem, literature review-primary and secondary sources, reviews, monograph, patents, research databases, web as a source, searching the web, critical literature review, identifying gap areas from literature and research database, development of working hypothesis.

UNIT-II

DATA COLLECTION AND ANALYSIS: Accepts of method validation, observation and collection of data, methods of data collection, sampling methods, data processing and analysis strategies and tools,data analysis with statically package (Sigma STAT,SPSS for student t-test, ANOVA, etc.), hypothesis testing.

UNIT-III

SOFT COMPUTING: Computer and its role in research, Use of statistical software SPSS, GRETL etcin research. Introduction to evolutionary algorithms - Fundamentals of Genetic algorithms, Simulated Annealing, Neural Network based optimization, Optimization of fuzzy systems.

UNIT-IV

RESEARCH ETHICS, IPR AND SCHOLARY PUBLISHING: Ethics-ethical issues, ethical committees (human & animal); IPR- intellectual property rights and patent law, commercialization, copy right, royalty, trade related aspects of intellectual property rights (TRIPS); scholarly publishing-IMRAD concept and design of research paper, citation and acknowledgement, plagiarism, reproducibility and accountability.

UNIT-V

INTERPRETATION AND REPORT WRITING: Meaning of Interpretation, Technique of Interpretation, Precaution in Interpretation, Significance of Report Writing, Different Steps in Writing Report, Layout of the Research Report, Types of L T P C 45 15 0 4 Reports, Oral Presentation, Mechanics of Writing a Research Report, Precautions for Writing Research Reports, Conclusions.

Text Books:

1. Garg, B.L., Karadia, R., Agarwal, F. and Agarwal, U.K., 2002. An introduction to Research Methodology, RBSA Publishers.
2. Kothari, C.R., 1990. Research Methodology: Methods and Techniques. New Age International. 418p.
3. Sinha, S.C. and Dhiman, A.K., 2002. Research Methodology, Ess Ess Publications. 2 volumes.
4. Trochim, W.M.K., 2005. Research Methods: the concise knowledge base, Atomic Dog Publishing. 270p. . Wadehra, B.L. 2000. Law relating to patents, trade marks, copyright designs and geographical indications. Universal Law Publishing.

MT-3.4: CRYPTOGRAPHY & NETWORK SECURITY

Objective:

- Learn fundamentals of cryptography and its application to network security.
- Understand network security threats, security services, and countermeasures.
- Acquire background on well-known network security protocols such.
- Understand vulnerability analysis of network security.

Learning Outcome:

At the end of this course student will be able to:

- Understand various Cryptographic Techniques
- Apply various public key cryptography techniques
- Implement Hashing and Digital Signature techniques
- Implement system level security applications

UNIT-I

Overview of Cryptography, Substitution and affine cipher and their cryptanalysis, Perfect Security, Block Cipher, Data Encryption Standard (DES), Differential and linear Cryptanalysis, Block Cipher Design Principles, Block Cipher modes of operation, Advanced Encryption Standard.

UNIT-II

Principles of Public-Key Cryptosystems, The RSA Algorithm, Key Management, Diffie-Helman Key Exchange, Authentication Functions, Message Authentication Codes (MAC), Hash Functions, Security of Hash Functions and MAC, Secure Hash Algorithm, HMAC.

UNIT-III

Discrete Logarithms, ElGamal System, Schnorr signature scheme, The ElGamal signature scheme, The digital signature algorithm, Provable secure signature schemes.

UNIT-IV

Elliptic curve over the reals, Elliptic curves modulo a prime, Properties of Elliptic cures Point compression and ECIes, Computing point multiples on Elliptic curves, Elliptic curve digital signature algorithm, Elliptic curve factorization, Elliptic curve primality test.

UNIT-V

Network Security Practice: Kerberos, X.509 Authentication Service, Public Key Infrastructure, E-Mail Security (Pretty Good Privacy), IP Security (Architecture, Authentication Header, Encapsulation Security Payload, Combining Security Associations, Key Management), Web Security (Secure Sockets Layer and Transport Layer Security).

Text Books:

1. W. Stallings – Cryptography and Network Security Principles and Practice, Pearson Education Asia, 3rd Edition, 2000. Ch. [1, 3, 5, 9, 10 (10.1, 10.2), 11, 12 (12.2, 12.4), 13 (13.3), 14, 15, 16, 17].
2. D. Stinson - Cryptography : Theory and Practice, CRC Press, 2006, Ch. [1, 2 (2.3), 6, 7, 12]
3. Behrouz A. Frouzan: Cryptography and Network Security, TMH
4. B. Schmeier – Applied Cryptography, New York, Wiley, 1996.
5. N. Koblitz – A Course in Number Theory and Cryptography, Springer Verlag