KONGU ENGINEERING COLLEGE, PERUNDURAI, ERODE – 638 052
(An Autonomous Institution affiliated to Anna University Chennai)

M.TECH. DEGREE IN INFORMATION TECHNOLOGY
(Information and Cyber Warfare)
(FULL TIME)

CURRICULUM

(For the candidates admitted from academic year 2013 – 14 onwards)

SEMESTER - I

Course Code	Course Title	Hours/ Week			Credit	Maximum Marks		
		L	T	P		CA	ESE	Total
	THEORY							
11MI101	Mathematical Foundations of Information Security	3	1	0	4	50	50	100
11MI102	Advanced Data Structures and Algorithms	3	1	0	4	50	50	100
11MI103	Advanced Database Technology	3	0	0	3	50	50	100
11MI104	Distributed Operating Systems	3	0	0	3	50	50	100
11MI105	Secure Software Engineering	3	0	0	3	50	50	100
11MI106	Information Theory and Coding	3	0	0	3	50	50	100
	PRACTICAL							
11MI107	Cryptography and Database Security Laboratory	0	0	3	1	100	0	100
11MI108	Advanced Data Structures and Operating System Laboratory	0	0	3	1	100	0	100
				Total	**22**			

CA - Continuous Assessment, ESE – End Semester Examination

KONGU ENGINEERING COLLEGE, PERUNDURAI, ERODE – 638 052
(An Autonomous Institution affiliated to Anna University Chennai)

M.TECH. DEGREE IN INFORMATION TECHNOLOGY
(Information and Cyber Warfare)
(FULL TIME)

CURRICULUM

(For the candidates admitted from academic year 2013 – 14 onwards)

SEMESTER - II

Course Code	Course Title	Hours/ Week			Credit	Maximum Marks		
		L	T	P		CA	ESE	Total
	THEORY							
11MI201	Cyber Forensics	3	0	0	3	50	50	100
11MI202	Cyber Law and Security Policies	3	0	0	3	50	50	100
11MI203	Distributed Systems Security	3	0	0	3	50	50	100
11MI204	Advanced Wireless Technologies	3	0	0	3	50	50	100
	Elective – I	3	0	0	3	50	50	100
	Elective – II	3	0	0	3	50	50	100
	PRACTICAL							
11MI205	Advanced Wireless Networks Laboratory	0	0	3	1	100	0	100
11MI206	Distributed Systems Laboratory	0	0	3	1	100	0	100
				Total	**20**			

CA – Continuous Assessment, ESE – End Semester Examination

KONGU ENGINEERING COLLEGE, PERUNDURAI, ERODE – 638 052
(An Autonomous Institution affiliated to Anna University Chennai)

M.TECH. DEGREE IN INFORMATION TECHNOLOGY
(Information and Cyber Warfare)
(FULL TIME)

CURRICULUM
(For the candidates admitted from academic year 2013 – 14 onwards)

SEMESTER – III

Course Code	Course Title	Hours / Week			Credit	Maximum Marks		
		L	T	P		CA	ESE	Total
	THEORY							
	Elective – III	3	0	0	3	50	50	100
	Elective - IV	3	0	0	3	50	50	100
	Elective - V	3	0	0	3	50	50	100
	PRACTICAL							
11MI301	Project Work - Phase I	0	0	12	6	50	50	100
				Total	**15**			

CA – Continuous Assessment, ESE – End Semester Examination

SEMESTER - IV

Course Code	Course Title	Hours / Week			Credit	Maximum Marks		
		L	T	P		CA	ESE	Total
	PRACTICAL							
11MI401	Project Work - Phase II	0	0	24	12	100	100	200
				Total	**12**			

CA- Continuous Assessment, ESE – End Semester Examination

LIST OF ELECTIVES					
Course Code	Course Title	L	T	P	C
11MI011	Computer Security, Audit Assurance and Risk Management	3	0	0	3
11MI012	Information Retrieval Techniques	3	0	0	3
11MI013	Social Network Analysis	3	0	0	3
11MI014	Secured Network Protocols	3	0	0	3
11MI015	Steganography and Digital Watermarking	3	0	0	3
11MI016	Secured Architectures	3	0	0	3
11MI017	Video Analytics	3	0	0	3
11MI018	Ethical Hacking	3	0	0	3
11MI019	Game Theory	3	0	0	3
11MI020	Biometric Security	3	0	0	3
11MI021	Unix Internals	3	0	0	3
11MI022	Secure Cloud Computing	3	0	0	3
11MS014	XML and Web Services	3	0	0	3
11MI023	Security Threats	3	0	0	3
11MI024	Dependable Distributed Systems	3	0	0	3
11MI025	Access Control and Identity Management System	3	0	0	3
11MI026	Object Oriented Software Engineering	3	0	0	3
11MI027	Adhoc and Wireless Sensor Networks	3	0	0	3
11MI028	Cyber Physical Systems	3	0	0	3

11MI101 MATHEMATICAL FOUNDATIONS OF INFORMATION SECURITY

3 1 0 4

Objectives:

On completion of the course the students are expected

- To understand the concepts of number theory
- To know the properties and applications of number theory.
- To implement number theory concepts into simple and public key cryptosystems.

15

MODULE – I

Elementary Number Theory: O and Ω notations – time estimates for doing arithmetic –divisibility and the Euclidean algorithm – Congruences: Definitions and properties – linear congruences, residue classes, Euler's phi function – Fermat's Little Theorem – Chinese Remainder Theorem – Applications to factoring – groups, rings, finite fields – quadratic residues and reciprocity: Quadratic residues – Legendre symbol – Jacobi symbol- Hash and MAC algorithms.(Theorems without proof)

15

MODULE– II

Simple Cryptosystems: Enciphering Matrices – Encryption Schemes – Symmetric and Asymmetric Cryptosystems – Cryptanalysis – Block ciphers –Use of Block Ciphers – Multiple Encryption – Stream Ciphers –Affine cipher – Vigenere, Hill and Permutation Cipher – Secure Cryptosystem – Advanced Encryption Standard(AES) – Data Encryption Standard.

Public Key Cryptosystems: The idea of public key cryptography – The Diffie–Hellman Key Agreement Protocol - RSA Cryptosystem – Bit security of RSA – ElGamal Encryption-Digital signature standard – Discrete Logarithm – Knapsack problem – Zero-Knowledge Protocols – From Cryptography to Communication Security - Oblivious Transfer.(Theorems without proof)

15

MODULE–III

Primality and Factoring: Pseudoprimes – the rho (γ) method – Format factorization and factor bases – the continued fraction method – the quadratic seieve method.

Number Theory and Algebraic Geometry: Elliptic curves – basic facts – elliptic curve cryptosystems – elliptic curve primality test – elliptic curve factorization – elliptic curve confidentiality and signature.(Theorems without proof)

Lecture: 45, Tutorial: 15, TOTAL: 60

REFERENCE BOOKS

1. Neal Koblitz, "A Course in Number Theory and Cryptography", Second Edition, Springer, 2002.
2. Johannes A. Buchman, "Introduction to Cryptography", Second Edition, Springer, 2004.
3. Serge Vaudenay, "Classical Introduction to Cryptography – Applications for Communication Security", Springer, 2006.
4. Victor Shoup, "A Computational Introduction to Number Theory and Algebra", Cambridge University Press, 2005.
5. A. Manezes, P. Van Oorschot and S. Vanstone, "Hand Book of Applied Cryptography", CRC Press, 1996.
6. S.C. Coutinho, "The Mathematics of Ciphers – Number Theory and RSA Cryptography",A.K. Peters, Natick, Massachusetts, 1998.

11MI102 ADVANCED DATA STRUCTURES AND ALGORITHMS

3 1 0 4

Objectives:

On completion of the course the students are expected

- To know the basic data structures used in software development, along with algorithms for inserting, sorting and accessing data
- To create and use the data structures and know the best situations for each, depending on the type of data to be stored and the running time (computational complexity) of algorithms for insertion, sorting and retrieval.

MODULE – I **15**

Trees and Sorting: Mathematical Induction - Asymptotic Notations – Algorithm Analysis - NP-Hard and NP-Completeness – Recurrence Equations – Solving Recurrence Equations – Memory Representation of Multi-dimensional Arrays – Time-Space Tradeoff - Heapsort – Quicksort – Topological sort - Sorting in Linear Time – Elementary Data Structures –Hash Tables – Binary Search Trees – AVL Trees – Red-Black trees – Multi-way Search Trees – B-Trees- Fibonacci Heaps – Data Structures for Disjoint Sets.

MODULE– II **15**

Graphs and Algorithm Design Techniques: Divide-and-Conquer – Greedy – Dynamic Programming – Amortized Analysis - Backtracking – Branch-and-Bound techniques-Elementary graph Algorithms – Minimum Spanning Trees – Single-Source Shortest Paths- All-Pairs Shortest Paths – Maximum Flow - multithreaded Algorithms – Matrix Operations.

MODULE–III **15**

Linear Programming: Linear programming – Polynomials and FFT – Computational Geometry – NP-Completeness – Approximation Algorithms.

Lecture : 45, Tutorial : 15, TOTAL : 60

REFERENCE BOOKS

1. Thomas H. Coreman, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein, “Introduction to Algorithms”, PHI, 3rd Edition, 2010.
2. G. Brassard and P. Bratley, “Algorithmics: Theory and Practice”, Printice –Hall, 1997.
3. E. Horowitz, S.Sahni and Dinesh Mehta, “Fundamentals of Data structures in C++”, University Press,2007.
4. E. Horowitz, S. Sahni and S. Rajasekaran, “Computer Algorithms/C++”, 2 nd Edition, University Press, 2007.

5 Alfred V. Aho, Jeffrey D. Ullman, John E. Hopcroft, “Data Structures and Algorithms”, Addison Wesley 1983.

11MI103 ADVANCED DATABASE TECHNOLOGY

3 0 0 3

Objectives:

On completion of the course the students are expected

- To know the fundamentals of relational and object databases
- To make a study of optimization based on cost and size of the databases
- To understand the concepts of distributed databases and concurrency control
- To implement security services on databases.

MODULE – I 15

Relational Data Model – SQL - Database Design - Entity-Relationship Model – Relational Normalization – Embedded SQL – Dynamic SQL – JDBC – ODBC- Case Studies -Object Databases - Conceptual Object Data Model – XML and Web Data – XML Schema – Distributed Data bases – Parallel databases-OLAP and Data Mining – ROLAP and MOLAP- Case Studies

MODULE– II 15

Processing Basics – Heuristic Optimization – Cost, Size Estimation - Models of Transactions – Architecture – Transaction Processing in a Centralized and Distributed System – TP Monitor-Case Studies for Real time Systems- Information retrieval

Schedules – Concurrency Control – Objects and Semantic – Locking – Crash, Abort and Media, Failure – Recovery – Atomic Termination – Distributed Deadlock – Global Serialization – Replicated Databases – Distributed Transactions in Real World - Case Studies

MODULE–III 15

Security – Encryption – Digital Signatures – Authorization – Authenticated RPC - Integrity - Consistency - Database Tuning - Optimization and Research Issues - Case Studies

Advanced Topics – Advanced application development- Spatial and Temporal data and mobility- Advanced transaction processing

TOTAL: 45

REFERENCE BOOKS

1. Philip M. Lewis, Arthur Bernstein and Michael Kifer, “Databases and Transaction Processing: An Application-Oriented Approach”, Addison-Wesley, 2002.
2. R. Elmasri and S.B. Navathe, “Fundamentals of Database Systems”, 3rd Edition, Addison Wesley,2004.
3. Abraham Silberschatz, Henry. F. Korth and S.Sudharsan, “Database System Concepts”,6th Edition, Tata McGraw Hill, 2011.
4. Raghu Ramakrishnan and Johannes Gehrke, “Database Management Systems”, 3rd Edition, TMH, 2003

11MI104 DISTRIBUTED OPERATING SYSTEMS

3 0 0 3

Objectives:

On completion of the course the students are expected

- To become familiar with the fundamental concepts of distributed operating systems
- To become competent in recognizing operating systems features and issues
- To understand operating system design and how it impacts application systems design and performance.

MODULE – I **15**

Process synchronization: Functions of an Operating System – Design Approaches –Types of Advanced Operating Systems- synchronization mechanisms- process deadlocks**:** Preliminaries – Models of Deadlocks – Models of Resources – A Graph-Theoretic Model of a System State – Necessary and Sufficient Conditions for a Deadlock – Systems with Single Unit-Requests – Systems with only Consumable Resources – Systems with only Reusable Resources

Distributed Operating System: Architecture of distributed systems-Theoretical foundations: Inherent Limitations of a Distributed System – Lamport's Logical clocks – Vector Clocks – Casual Ordering of Messages – Global State – Cuts of a Distributed Computation – Termination Detection Distributed mutual exclusion -Distributed deadlock detection-agreement protocols: The System Model – A Classification of Agreement Problems – Solutions to the Byzantine Agreement Problem – Applications of Agreement Algorithms

MODULE– II **15**

Distributed resource management: Distributed file systems – Architecture – Mechanisms for Building Distributed File Systems – Design Issues – Case Studies – Log-Structured File Systems-Distributed shared memory**:** Architecture and Motivation – Algorithm for Implementing DSM – Memory Coherence Protocols – Design Issues – Case Studies-Distributed scheduling**:** Motivation – Issues in Load Distributing – Components of a Load Distributing Algorithm – Stability – Load Distributing Algorithm – Performance Comparison – Selecting a Suitable Load Sharing Algorithm – Requirements for Load Distributing – Load Sharing Policies – Task Migration – Issues in Task Migration

Failure recovery and fault tolerance: Basic Concepts – Classification of Failures – Backward and Forward Error Recovery – Backward Error Recovery :Basic Approaches – Recovery in Concurrent Systems – Consistent Set of Check points – Synchronous Check pointing and Recovery – Asynchronous Check pointing and Recovery – Check pointing for Distributed Database Systems - Recovery in Replicated Distributed Database Systems-Fault tolerance: Issues – Atomic Actions and Committing – Commit Protocols – Nonblocking Commit Protocols – Voting Protocols – Dynamic Voting Protocols – The Majority based Dynamic Voting Protocols – Failure Resilient Processes – Reliable Communication.

MODULE–III **15**

Multiprocessor operating systems: Multiprocessor system architectures- Basic Multiprocessor System Architectures – Interconnection Networks for Multiprocessor Systems – Caching – Hypercube Architectures-multiprocessor operating systems **:** Structures of Multiprocessor Operating Systems – Operating System Design Issues – Process Synchronization – Process Scheduling – Memory Management: The Mach Operating System – Reliability / Fault Tolerance: The Sequoia System

Database operating systems: Requirements of a Database Operating System -concurrency control**:** A Concurrency Control Model of Database Systems – Serializability Theory – Distributed Database Systems- concurrency control algorithms: Introduction – Basic Synchronization Primitives – Lock Based Algorithms – Time Stamp Based Algorithms – Optimistic Algorithms – Concurrency Control Algorithms: Data Replication.

TOTAL: 45

REFERENCE BOOKS

1. Mukesh Singhal, “Advanced concepts in operating systems”, Tata McGraw Hill , 2008
2. Tanenbaum, Andrew S.,” Modern Operating Systems”, Third Edition , Prentice Hall , 2008
3. Tanenbaum Andrew S,Albert S Woodhull, “Operating Systems Design and Implementation”, Third Edition, Prentice Hall, 2006.
4. Sinha, Pradeep K. “Distributed Operating System: Concepts and Design”, IEEE Computer Society Press, PHI, 2004.
5. Tanenbaum, Andrew S., “Modern Operating Systems”, Second Edition, Pearson Education, New Delhi, 2004.

11MI105 SECURE SOFTWARE ENGINEERING

3 0 0 3

Objectives:

On completion of the course the students are expected

- To get familiarized with the concepts of secure software architecture
- To know about the concepts of tools used in architectural design.

MODULE – I 15

Problem, Process, and Product - Problems of software practitioners – approach through software reliability engineering- experience with SRE – SRE process – defining the product – Testing acquired software – reliability concepts- software and hardware reliability - Implementing Operational Profiles - Developing, identifying, creating, reviewing the operation – concurrence rate – occurrence probabilities- applying operation profiles

Engineering "Just Right" Reliability - Defining "failure" for the product - Choosing a common measure for all associated systems. - Setting system failure intensity objectives –Determining user needs for reliability and availability - overall reliability and availability objectives, common failure intensity objective - Developed software failure intensity objectives – Engineering software reliability strategies - Preparing for Test - Preparing test cases - Planning number of new test cases for current release - Allocating new test cases - Distributing new test cases among new operations - Detailing test cases - Preparing test procedures

MODULE– II 15

Executing Test - Planning and allocating test time for the current release - Invoking test identifying - identifying failures - Analyzing test output for deviations – Determining which deviations are failures - Establishing when failures occurred - Guiding Test - Tracking reliability growth - Estimating failure intensity - Using failure intensity patterns to guide test – Certifying reliability - Deploying SRE - Core material - Persuading your boss, your coworkers, and stakeholders - Executing the deployment - Using a consultant

Using UML for Security - UML diagrams for security requirement - security business process physical security - security critical interaction - security state - Analyzing Model - Notation - formal semantics - security analysis - important security opportunities - Model based security engineering with UML - UML SEC profile- Design principles for secure systems – Applying security patterns

MODULE–III 15

Applications - Secure channel - Developing Secure Java program- more case studies - Tool support for UML SEC - Extending UML CASE TOOLS with analysis tools - Automated tools for UML SEC - Formal Foundations - UML machines - Rely guarantee specifications- reasoning about security properties

TOTAL: 45

REFERENCE BOOKS

1. John Musa D, "Software Reliability Engineering", 2nd Edition, Tata McGraw-Hill, 2005 (MODULE I and II)
2. Jan Jürjens, "Secure Systems Development with UML", Springer; 2004 (MODULE II and III)

11MI106 INFORMATION THEORY AND CODING

3 0 0 3

Objectives:

On completion of the course the students are expected

- To understand the concepts of probability theory and random variables
- To explore memory-less finite schemes and continuous channels
- To understand the elements of encoding and types of encoding

MODULE – I **15**

Source Coding - Introduction to information theory, uncertainty and information, average mutual information and entropy, source coding theorem, Shannon-fano coding, Huffman coding, Arithmetic coding, Lempel-Ziv algorithm, run-length encoding and rate distortion function.

Channel capacity and coding - channel models, channel capacity, channel coding, information capacity theorem, random selection of codes - Error control coding: linear block codes and their properties, decoding of linear block code, perfect codes, hamming codes, optimal linear codes and MDS codes.

MODULE - II **15**

Cyclic codes - polynomials, division algorithm for polynomials, a method for generating cyclic codes, matrix description of cyclic codes, burst error correction, fire codes, golay codes, CRC codes, circuit implementation of cyclic codes - BCH codes: minimal polynomials, generator polynomial for BCH codes, decoding of BCH codes, Reed-Solomon codes and nested codes.

Convolutional codes - tree codes and trellis codes, polynomial description of convolutional codes, distance notions for convolutional codes, generation function, matrix description of convolutional codes, viterbi decoding of convolutional codes, distance bounds for convolutional codes, turbo codes and turbo decoding.

MODULE- III **15**

Trellis Coded Modulation - concept of coded modulation, mapping by set partitioning, ungerboeck's TCM design rules, TCM decoder, Performance evaluation for Additive White Gaussian Noise (AWGN) Channel, TCM for fading channels.

TOTAL : 45

REFERENCE BOOKS

1. Ranjan Bose, "Information theory, coding and cryptography", Tata McGraw Hill, 2002.
2. Viterbi, "Information theory and coding", McGraw Hill, 1982.
3. John G. Proakis, "Digital Communications", 2nd Edition, McGraw Hill, 1989.

11MI107 CRYPTOGRAPHY AND DATABASE SECURITY LABORATORY

0 0 3 1

Objectives:

On completion of the course the students are expected

- To understand the concepts of security mechanisms, various types of attacks and implement various algorithms using Sender and Receiver approach
- To write and execute various types of database queries, procedures, functions and triggers
- To develop mini projects which include E-R model design, Input validation, modules design and report generation

LIST OF EXPERIMENTS /EXERCISES

1. Implementation of Ceaser cipher with Brute force attack, one time pad, poly alphabetic cipher
2. Implementation of Permutation and Transposition Techniques
3. Implementation of Random number generator, Fermat's theorem, Euler's theorem , Euclidian algorithm , Extended Euclidian algorithm and CRT
4. Implementation of Miller Rabin Primality test and identifying the weakness of the test
5. Implementation of RSA and Diffie Hellman key exchange
6. Implementation of Data Definition Language (DDL) commands , Data Manipulation Language (DML) and Data Control Language (DCL) commands in RDBMS
7. Implementation of all Join operations and Integrity Constraints, High-level language extension with Cursors and Triggers
8. Implementation of Procedures , Functions and Embedded SQL
9. Implementation of SQL attack , DB attack, session hijack attack and preventing these attacks
10. Mini project (Application Development using Oracle/ MYSQL)
    - Inventory Control System.
    - Hospital Management System.
    - Railway Reservation System.
    - Web Based User Identification System.
    - Hotel Management System.
    - Student Information System

REFERENCES / MANUALS/SOFTWARE:

Linux and C

Front End :Microsoft Visual Studio 6.0, Microsoft .NET Framework SDK v2.0

Back End :ORACLE / SQL SERVER

11MI108 ADVANCED DATASTRUCTURES AND OPERATING SYSTEMS LABORATORY

0 0 3 1

Objectives:

On completion of the course the students are expected

- To implement the various data structures concepts
- To implement and simulate operating system concepts

LIST OF EXPERIMENTS /EXERCISES

1. Represent a polynomial as a linked list and write functions for polynomial Addition
2. Implement stack and use it to evaluate the arithmetic expression
3. Implement an expression tree. Produce its pre-order, in-order, and post-order traversals.
4. Implement Prim's algorithm using priority queues to find MST of an undirected graph
5. Implement insertion and deletion in AVL trees
6. Implement the Quick Sort and Heap Sort
7. Given the list of processes, their CPU burst times and arrival times, display/print the Gantt chart for FCFS and SJF. For each of the scheduling policies, compute and print the average waiting time and average turnaround time
8. Given the list of processes, their CPU burst times and arrival times, display/print the Gantt chart for Priority and Round robin. For each of the scheduling policies, compute and print the average waiting time and average turnaround time
9. Implement the Producer – Consumer problem using semaphores
10. Implement Banker’s Algorithm
11. Implement Best-fit, First-fit algorithms for memory management
12. Implement FIFO and LRU page replacement algorithms

REFERENCES / MANUALS/SOFTWARE:

Linux and C

11MI201 CYBER FORENSICS

3 0 0 3

Objectives:

On completion of the course the students are expected

- To know the fundamentals of computer forensics.
- To have an overview of techniques for Data Recovery and Evidence Collection.
- To know various threats associated with security and information warfare.
- To know the tools and tactics associated with cyber forensics.

MODULE – I **15**

Introduction: Computer Forensics Fundamentals – Types of Computer Forensics Technology – Types of Vendor and Computer Forensics Services.

Computer forensics evidence capture: Data Recovery – Evidence Collection and Data Seizure – Duplication and Preservation of Digital Evidence - Computer Verification and Authentication.

MODULE - II **15**

Computer forensics analysis: Discovery of Electronic Evidence – Identification of Data – Reconstructing Past Events - Fighting against Macro Threats – Information Warfare Arsenal – Tactics of the Military – Tactics of Terrorist and Rogues – Tactics of Private Companies.

Information warfare: Arsenal – Surveillance Tools – Hackers and Theft of Components – Contemporary computer Crime Identity - Theft and Identity Fraud – Organized Crime & Terrorism Avenues - Prosecution and Government Efforts – Applying the First Amendment to Computer Related Crime – The Fourth Amendment and Other Legal Issues.

MODULE - III **15**

Computer forensics cases: Developing Forensic Capabilities – Searching and Seizing Computer Related Evidence – Processing Evidence and Report Preparation – Conclusions and Future Issues.

TOTAL : 45

REFERENCE BOOKS

1. John R. Vacca, "Computer Forensics: Computer Crime Scene Investigation, Volume 1 Cengage Lear, 2005.
2. Marjie T Britz, "Computer Forensics and Cyber Crime: An Introduction, 2/e, Pearson Education ISBN: 9788131764015.
3. Marie-Helen Maras, "Computer Forensics: Cybercriminals, Laws and Evidence", Jones & Bartlett Publishers, 2011.
4. Chad Steel, "Windows Forensics", Wiley India, 2006.
5. Majid Yar, "Cybercrime and Society", Sage Publications, 2006.
6. Robert M Slade, "Software Forensics", Tata McGraw Hill, 2004.

11MI202 CYBER LAW AND SECURITY POLICIES

3 0 0 3

Objectives:

On completion of the course the students are expected

- To know about security standards and how to secure the system.
- To explore various security policies and employee responsibilities.
- To understand the significance of information security.

MODULE – I **15**

Introduction to Computer Security: Definition, Threats to security, Government requirements, Information Protection and Access Controls, Computer security efforts, Standards, Computer Security mandates and legislation, Privacy considerations, International security activity.

Secure System Planning and administration: Introduction to the orange book, Security policy requirements, accountability, assurance and documentation requirements, Network Security, The Red book and Government network evaluations.

MODULE– II **15**

Information security policies and procedures: Corporate policies- Tier 1, Tier 2 and Tier 3 policies - process management-planning and preparation-developing policies-asset classification policy-developing standards.

Information security: fundamentals-Employee responsibilities- information classification-Information handling- Tools of information security- Information processing-secure program administration.

MODULE–III **15**

Organizational and Human Security: Adoption of Information Security Management Standards, Human Factors in Security- Role of information security professionals.

TOTAL : 45

REFERENCE BOOKS

1. Debby Russell and Sr. G.T Gangemi, "Computer Security Basics (Paperback)”, 2nd Edition, O’ Reilly Media, 2006.
2. Thomas R. Peltier, “Information Security policies and procedures: A Practitioner’s Reference”, 2nd Edition Prentice Hall, 2004.
3. Kenneth J. Knapp, “Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions”, IGI Global, 2009.
4. Thomas R Peltier, Justin Peltier and John blackley, ”Information Security Fundamentals”, 2nd Edition, Prentice Hall, 1996
5. Jonathan Rosenoer, “Cyber law: the Law of the Internet”, Springer-verlag, 1997.

11MI203 DISTRIBUTED SYSTEMS SECURITY

3 0 0 3

Objectives:

On completion of the course the students are expected

- To understand the various types of virus and related threats.
- To analyze various security attacks and virtualization techniques.
- To deploy architecture to provide service level solutions.

MODULE – I **15**

Introduction – Distributed Systems, Distributed Systems Security. Security in Engineering: Secure Development Lifecycle Processes - A Typical Security Engineering Process – Security Engineering Guidelines and Resources - Common Security Issues and Technologies: Security Issues, Common Security Techniques.

Host-level Threats and Vulnerabilities: Transient code Vulnerabilities - Resident Code Vulnerabilities - Malware: Trojan Horse – Spyware - Worms/Viruses – Eavesdropping – Job Faults - Infrastructure - Level Threats and Vulnerabilities: Network-Level Threats and Vulnerabilities - Grid Computing Threats and Vulnerabilities – Storage Threats and Vulnerabilities – Overview of Infrastructure Threats and Vulnerabilities

.

MODULE– II **15**

Application-Level Threats and Vulnerabilities: Application-Layer Vulnerabilities –Injection Vulnerabilities - Cross-Site Scripting (XSS) - Improper Session Management - Improper Error Handling - Improper Use of Cryptography - Insecure Configuration Issues - Denial of Service - Canonical Representation Flaws - Overflow Issues - Service-Level Threats and Vulnerabilities: SOA and Role of Standards - Service-Level Security Requirements - Service-Level Threats and Vulnerabilities - Service-Level Attacks - Services Threat Profile

Host-Level Solutions: Sandboxing – Virtualization - Resource Management - Proof-Carrying Code - Memory Firewall – Antimalware - Infrastructure-Level Solutions: Network-Level Solutions - Grid-Level Solutions - Storage-Level Solutions - Application-Level Solutions: Application-Level Security Solutions

MODULE–III **15**

Service-Level Solutions: Services Security Policy - SOA Security Standards Stack – Standards in Dept - Deployment Architectures for SOA Security - Managing Service-Level Threats - Compliance in Financial Services **-** SOX Compliance - SOX Security Solutions – Multilevel Policy-Driven Solution Architecture - Case Study: Grid **-** The Financial Application – Security Requirements Analysis- Future Directions **-** Cloud Computing Security – Security Appliances **-** Usercentric Identity Management **-** Identity-Based Encryption (IBE) **-** Virtualization in Host Security

TOTAL: 45

REFERENCE BOOKS

1. Abhijit Belapurakar, Anirban Chakrabarti and et al., “Distributed Systems Security: Issues , Processes and solutions”, Wiley, Ltd., Publication, 2009.
2. Abhijit Belapurkar, Anirban Chakrabarti, Harigopal Ponnapalli, Niranjan Varadarajan,Srinivas Padmanabhuni and Srikanth Sundarrajan, “Distributed Systems Security: Issues, Processes and Solutions”, Wiley publications, 2009.
3. Rachid Guerraoui and Franck Petit, “Stabilization, Safety, and Security of Distributed Systems”, Springer, 2010.

11MI204 ADVANCED WIRELESS TECHNOLOGIES

3 0 0 3

Objectives:

On completion of the course the students are expected

- To know various generations of wireless and cellular Networks.
- To know about fundamentals of 3G Services, its protocols and applications.
- To understand about evolution of 4G Networks, its architecture and applications.
- To know about WiMAX networks, protocol stack and standards.
- To understand about the emerging trends of smart phones and evolution of latest standards like DLNA and NFC.

MODULE – I **15**

Introduction and 3G Networks: History of mobile cellular systems - First Generation – Second Generation - Generation 2.5 - Overview of 3G & 4 G - 3GPP2 standards-3G Networks - Evolution from GSM - 3G Services & Applications - UMTS network structure - Core Network, UMTS Radio access – HSPA – HSUPA – HSDPA – CDMA 1X – EVDO Rev-0 – Rev- B – Rev-C Architecture – Protocol stack

.

MODULE– II **15**

4G LTE Networks and WIMAX Networks: LTE – Introduction – Radio interface architecture – Physical layer – Access procedures- System Architecture Evolution (SAE) - WiMAX – Introduction – IEEE 802.16 – OFDM – MIMO – IEEE 802.20

DLNA & NFC Revolution: Introduction & Evolution – Applications of DLNA and NFC – DLNA Architecture and Protocol stack - Smartphone and NFC – Mobile Commerce and NFC – NFC tags.

MODULE–III **15**

Wireless Standards and Policy Solutions: Security essentials – Information classification standards - Wireless Threats: Cracking WEP -Hacking Techniques- Wireless Attacks – Airborne Viruses– Network Solutions – Software Solutions – Physical Hardware Security- Wireless Security – Securing WLAN – Virtual Private Networks – Wireless Public Key infrastructure Tools – Auditing tools – Pocket PC hacking – wireless hack walkthrough.

Security analysis process and WLAN Configuration - Privacy in Wireless World – Legislation and Policy – Identify targets and roles analysis – Attacks and vulnerabilities – Analyze mitigations and protection- systematic exploitation of 802.11b WLAN – WEP – WEP Decryption script – overview of WEP attack –Implementation - Analyses of WEP attacks.

TOTAL : 45

REFERENCE BOOKS

1. Juha Korhonen, “Introduction to 3G Mobile Communication”, Artech House, (WWW.artechhouse.com), Jan 2003, ISBN-10 : 1580535070
2. Russel Dean Vines, “Wireless Security Essentials: Defending Mobile from Data Piracy”, John Wiley & Sons, 1st Edition, 2002
3. Cyrus, Peikari and Seth Fogie, “Maximum Wireless Security”, SAMS Publishing 2002.
4. Erik Dahiman, Stefan Parkvall, Johan Skold and Per Beming, “3G Evolution HSPA and LTE for Mobile Broadband”, Academic Press, Oct 2008, ISBN-10: 0123745381
5. Flavio Muratore, “UMTS Mobile Communication for the Future”, John Wiley & Sons Ltd, Jan 2001, ISBN-10: 0471498297
6. Harri Holma and Antti Toskala, “HSDPA/HSUPA for UMTS”, Johan Wiley & Sons Ltd, May 2006, ISBN- 10: 0470018844
7. Vijay K Garg , “ Wireless communications and Networking” , Morgan Kafmann Publishers, 2007, ISBN - 978-0-12-373580-5

11MI205 ADVANCED WIRELESS NETWORKS LABORATORY

0 0 3 1

Objectives:

On completion of the course the students are expected

- To know about various wireless protocols , energy model and security attacks

LIST OF EXPERIMENTS /EXERCISES

1. Simulation and performance analysis of various protocols in Wired Network
2. Simulation and performance analysis of AdHoc Network
3. Simulation and performance analysis of Distance Vector , DSR and AODV routing protocols
4. Simulation and performance analysis of IEEE 802.11 MAC protocol
5. Simulation and performance analysis of Wireless sensor Network using SMAC and Zigbee
6. Simulation and performance analysis of Energy model in Adhoc Networks
7. Simulation and performance analysis of Vehicular AdHoc Network
8. Simulation and performance analysis of Worm hole and Black hole attacks
9. Simulation of Web Cache in AdHoc Network
10. Simulation of Satellite Netwoking

REFERENCES / MANUALS/SOFTWARE:

NS2 software and AWK script

11MI206 DISTRIBUTED SYSTEMS LABORATORY

0 0 3 1

Objectives:

On completion of the course the students are expected

- To know the concepts of RMI and RMI-IIOP
- To explore the client and server side components of Java Technology
- To develop web applications in MVC architecture
- To conduct simple experiments in CORBA
- To explore the advanced concepts DII and DSI

LIST OF EXPERIMENTS

1. To create virtual server in a host operating system
2. To create an application to demonstrate thread synchronization
3. To create an application to simulate deadlock
4. To create Producer-Consumer application for sharing memory
5. To create a confidentiality service for client server application using TCP/ UDP sockets
6. To create a authentication service for client server application using TCP/UDP sockets
7. To create a multicast group for receiving messages using IP Multicasting
8. To create a simple RMI application for downloading files
9. To create a session bean for banking operations using JNDI
10. To develop an ORB application for share market information

REFERENCES / MANUALS/SOFTWARE

JDK 1.4 and above
Blazix Web and Application server
Visi Broker

11MI011 COMPUTER SECURITY, AUDIT ASSURANCE AND RISK MANAGEMENT

3 0 0 3

Objectives:

On completion of the course the students are expected

- To understand the concepts of public key encryption and firewalls
- To get familiarized with security assessment and auditing.
- To explore threat assessment and risk management.

MODULE – I **15**

Essentials of computer security - Sources of security threats – Intruders, Viruses, Worms and related threats - Threat identification - Threat analysis - Vulnerability identification and Assessment - Components of Computer Security - Physical security – System access control - Goals of Security - Efforts to secure computer networks – Ethical issues in Computer Security-Operational issues, Human issues - Intrusion Detection System (IDS) – Types and challenges – Intrusion prevention system (IPS) – Firewalls - Design Principles, Scanning, filtering and blocking

Essentials of Information Security – Introduction to Information Security- Need for Security- Legal, Ethical and Professional issues in Information Security

MODULE - II **15**

Vulnerabilities – Sources of vulnerabilities, Vulnerability identification and Assessment, Cyber crime and Hackers, Viruses and content filtering - Security Assessment, Analysis and Assurance – Computer network security protocol and standards - Security Policies – Integrity policies – confidentiality policies - Security models - Access Control Matrix Model, Take-Grant Protection Model.

Security Monitoring and Auditing - Assurance and Trust, Need for Assurance, Role of Requirements in Assurance, Audit Assurance in Software Development Phases, Building Secure and Trusted Systems - Designing an Auditing System, Implementation Considerations, Auditing to Detect Violations of a security Policy, Auditing Mechanisms, Audit Browsing.

MODULE -III **15**

Risk management and security planning – Risk management Process Overview- Cost-Benefit Analysis, Risk Analysis, Laws and Customs, Human Issues, Organizational issues – Information system Risk analysis – System approach to risk management, Threat assessment, Assets and safeguards, modes of risk analysis – Effective risk analysis, Qualitative Risk analysis, Value analysis

Trust Management and Privacy Policy: Trust management- trusted platforms- The persuasiveness of ambient intelligence-privacy policies

TOTAL : 45

REFERENCE BOOKS

1. Matt Bishop, “Computer Security: Art and Science”, Addison-Wesley Professional, 2003.
2. Michael E Whitman, “Principles of Information Security” fourth edition , Cengage learning, 2012
3. Milan Petkovic , “Security, Privacy and trust in modern data management”, Springer, 2007
4. Joseph M.Kizza, “Computer Network security”, Springer, 2005
5. Matt Bishop, “Introduction to Computer Security”, Addison-Wesley Professional, 2005.
6. Thomas R.Peltier, “Information Security Risk Analysis”, CRC Press, 2001.
7. C.A.Roper, “Risk management for Security professional”, Elsevier, 1999.

11MI012 INFORMATION RETRIEVAL TECHNIQUES

3 0 0 3

Objectives:

On completion of the course the students are expected

- To understand text retrieval models and pattern matching.
- To understand the process of human computer interaction.
- To explore web through various search engines.

MODULE–I 15

Introduction: Basic Concepts – Retrieval Process – Modeling – Classic Information Retrieval – Set Theoretic, Algebraic and Probabilistic Models – Structured Text Retrieval Models – Retrieval Evaluation –Word Sense Disambiguation

Querying: Languages – Key Word based Querying – Pattern Matching – Structural Queries – Query Operations – User Relevance Feedback – Local and Global Analysis – Text and Multimedia languages

MODULE– II 15

Text operations and user Interface : Document Preprocessing – Clustering – Text Compression - Indexing and Searching – Inverted files – Boolean Queries – Sequential searching – Pattern matching – User Interface and Visualization – Human Computer Interaction – Access Process – Starting Points –Query Specification - Context – User relevance Judgement – Interface for Search

Multimedia Information Retrieval: Data Models – Query Languages – Spatial Access Models – Generic Approach – One Dimensional Time Series – Two Dimensional Color Images – Feature Extraction

MODULE– III 15

Applications: Searching the Web – Challenges – Characterizing the Web – Search Engines – Browsing – Meta-searchers – Online IR systems – Online Public Access Catalogs – Digital Libraries – Architectural Issues – Document Models, Representations and Access – Prototypes and Standards

TOTAL: 45

REFERENCE BOOKS

1. Ricardo Baeza-Yate, Berthier Ribeiro-Neto, “Modern Information Retrieval”, Pearson Education Asia, 2005.
2. G.G. Chowdhury, “Introduction to Modern Information Retrieval”, Neal-Schuman Publishers; 2nd edition, 2003.
3. Daniel Jurafsky and James H. Martin, “Speech and Language Processing”, Pearson Education, 2000.
4. David A. Grossman, Ophir Frieder, “ Information Retrieval: Algorithms, and Heuristics”, Academic Press, 2000.
5. Charles T. Meadow, Bert R. Boyce, Donald H. Kraft, “Text Information Retrieval Systems”, Academic Press, 2000.

11MI013 SOCIAL NETWORK ANALYSIS

3 0 0 3

Objectives:

On completion of the course the students are expected

- To understand about semantic web and social networks
- To explore various social network infrastructures and communities
- To know about providing privacy in online social networks

MODULE – I **15**

Introduction to the semantic web and social networks: Limitations of the current Web – The Semantic Solution – Development of the Semantic Web - The emergence of the social web – Discussion-Development of Social Network Analysis – Key concepts and measures in network analysis

Web data and semantics in social network applications: Electronic discussion networks – Blogs and online communities – Web- based Networks- Ontologies and their role in the Semantic Web - Ontology languages for the Semantic Web-State-of-the-art in network data representation – Ontological representation of social relationships – Aggregating and reasoning with social network area- Building semantic web application with social network features – Flink: the social networks of the Semantic web community – open academia: distributed, semantic- based publication management

MODULE - II **15**

Evaluation of web-based social network extraction : Differences between survey methods and electronic data extraction – Context of the empirical study – Data collection- Preparing the data – Optimizing goodness of fit – Comparison across method and networks – Predicting the goodness of fit – Evaluation through analysis- Semantic-based social network analysis in the sciences - Ontologies - emergent semantics in folksonomy systems

Social media mining and search: Discovering Mobile Social Networks by Semantic Technologies – Online Identities and Social Networking – Detecting Communities in Social Networks – Concept of Discovery in Youtube.com using Factorization method – Mining Regional Representative Photos from Consumer – Generated Geotagged Photos – Collaborating Filtering Based on Choosing a Different Number of Neighbors for Each User – Discovering Communities from Social Networks : Methodologies and Applications

MODULE- III **15**

Social network infrastructures and communities: Decentralized Online Social Networks – Multi-Relational Characterization of Dynamic Social Networks Communities – Accessibility Testing of Social Websites – Understanding and Predicting Human Behavior for Social Communities – Associating Human – Centered Concepts with Social Networks Using Fuzzy Sets

Privacy in online social networks: Managing Trust in Online Social Networks – Security and Privacy in Online Social Networks – Investigation of Key-Player Problem in Terrorist Network Using Bayes Conditional Probability – Optimizing Targeting of Intrusion Detection System in Social Networks – Security Requirements for Social Networks in Web 2.0- visualization and applications of social networks

TOTAL : 45

REFERENCE BOOKS

1. Peter mika, "Social networks and the semantic web", Springer Publishers, 2007
2. Borko Furht, "Handbook of Social Network Technologies and Applications", Springer Publishers, 2010

11MI014 SECURED NETWORK PROTOCOLS

3 0 0 3

Objectives:

On completion of the course the students are expected

- To know about various network security protocols
- To get familiarized with wireless network standards.
- To get familiarized with global and mobile satellite systems

MODULE – I **15**

Local Area Network and LAN Protocols – ETHERNET Protocols – VLAN protocols – Wireless LAN Protocols – Metropolitan Area Network Protocol – Storage Area Network and SAN Protocols - FDMA, WIFI and WIMAX Protocols- security issues, Mobile IP – Mobile Support Protocol for IPv4 and IPv6 – Resource Reservation Protocol, Multi-casting Protocol – VGMP – IGMP – MSDP.

Network Security and Technologies and Protocols – AAA Protocols – Tunneling Protocols – Secured Routing Protocols – GRE- Generic Routing Encapsulation – IPSEC – Security architecture for IP – IPSECAH – Authentication Header – ESP – IKE – ISAKMP and Key management Protocol, IEEE 802.11 - Structure of 802.11 MAC – WEP- Problems with WEP – Attacks and Risk- Station security – Access point Security – Gate way Security – Authentication and Encryption.

MODULE - II **15**

Authentication and Network Security: Authentication requirements – Authentication functions – Message Authentication Codes – Hash Functions – Security of Hash Functions and MACs – MD5 message Digest algorithm - Secure Hash Algorithm – RIPEMD – HMAC- Authentication Applications: Kerberos – X.509 Authentication Service.

Security protocols – Transport layer protocols – SSL – Electronic mail security – PEM and S/MIME security protocol – Pretty Good Privacy – Web Security - Firewalls design principles –Trusted systems – Electronic payment protocols, Intrusion detection – password management – Viruses and related Threats – Virus Counter measures, Virtual Private Networks.

MODULE- III **15**

IEEE 802.15 and Bluetooth – WPAN Communication Protocols – IEEE 802.16- IEEE 802.16A- WCDMA – Services – WCDMA Products – Networks- device addressing – System Addressing – Radio Signaling Protocol – Multimedia Signaling Protocol.

Global Mobile Satellite Systems - Case studies of the IRIDIUM and GLOBALSTAR systems, Wireless Enterprise Networks: Introduction to Virtual Networks, Bluetooth technology, Bluetooth Protocols.

TOTAL : 45

REFERENCE BOOKS

1. Jawin, “Networks Protocols Handbook”, Jawin Technologies Inc., 2005.
2. William Stallings, “Cryptography and Network Security: Principles and Standards”, Prentice Hall India, 4th Edition, 2009.
3. Bruce Potter and Bob Fleck, “802.11 Security”, O’Reilly Publications, 2002.
4. Lawrence Harte, “Introduction to WCDMA”, Althos Publishing, 2004.
5. Yi-Bing Lin and Imrich Chlamtac, “Wireless and Mobile Networks Architectures”, John Wiley & Sons, 2001
6. Lawrence Harte, “Introduction to CDMA- Network services Technologies and Operations”, Althos Publishing, 2004.
7. Lawrence Harte, “Introduction to WIMAX”, Althos Publishing, 2005.

.

11MI015 STEGANOGRAPHY AND DIGITAL WATERMARKING

3 0 0 3

Objectives:

On completion of the course the students are expected

- To know about various steganography techniques.
- To analyze various water marking techniques.
- To get familiarized with various copyright laws.

MODULE – I **15**

Introduction to Information hiding – Brief history and applications of information hiding – Principles of Steganography – Frameworks for secret communication – Security of Steganography systems –Information hiding in noisy data – Adaptive versus non adaptive algorithms – Laplace filtering using cover models – Active and malicious attackers – Information hiding in written text – Examples of invisible communications.

Survey of steganographic techniques – Substitution system and bitplane tools – Transform domain techniques – Spread spectrum and information hiding – Statistical Steganography - Distortion and code generation techniques – Automated generation of English text.

MODULE - II **15**

Steganalysis – Detecting hidden information – Extracting hidden information - Disabling hidden information – Watermarking techniques – History – Basic Principles – applications – Requirements of algorithmic design issues – Evaluation and benchmarking of watermarking system.

Survey of current watermarking techniques – Cryptographic and psycho visual aspects – Choice of a workspace – Formatting the watermark bets - Merging the watermark and the cover – Optimization of the watermark receiver – Extension from still images to video – Robustness of copyright making systems

MODULE- III **15**

Fingerprints – Examples – Classification – Research history – Schemes – Digital copyright and watermarking – Conflict of copyright laws on the internet.

TOTAL : 45

REFERENCE BOOKS

1. Stefan Katzenbelsser and Fabien A. P. Petitcolas, “Information hiding techniques for Steganography and Digital Watermarking”, ARTECH House Publishers, January 2004.
2. Jessica Fridrich, “Steganography in Digital Media: Principles, Algorithms, and Applications”, Cambridge university press, 2010.
3. Abbas Cheddad, Vdm Verlag and Dr. Muller, “Digital Image Steganography” Aktienge sells chaft & Co. Kg, Dec 2009.
4. Ingemar Cox, Matthew Miller,Jeffrey Bloom,Jessica Fridrich and Ton Kalker, “Digital Watermarking And Steganography”, Morgan Kaufmann Publishers, Nov 2007.

11MI016 SECURED ARCHITECTURES

3 0 0 3

Objectives:

On completion of the course the students are expected

- To understand system level security architecture.
- To know middleware technologies and IDS.
- To analyze data management problem.

MODULE– I **15**

Architecture and Security - Architecture Reviews-Software Process-Reviews and the Software Development Cycle-Software Process and Architecture Models-Software Process and Security-Architecture Review of System-Security Assessments-Security Architecture Basics- Architecture Patterns in Security.

Low-Level Architecture - Code Review-importance of code review- Buffer Overflow Exploits-Countermeasures Against Buffer Overflow Attacks-patterns applicable- Security and Perl- Byte code Verification in Java-Good Coding Practices Lead to Secure Code- Cryptography- Trusted Code - Secure Communications.

MODULE– II **15**

Mid-Level Architecture - Middleware Security- Middleware and Security- The Assumption of Infallibility-The Common Object Request Broker Architecture-The OMG CORBA Security Standard-Vendor Implementations of CORBA Security-CORBA Security Levels-Secure Interoperability-Application-Unaware Security-Application-Aware Security-Application, Implications- Web Security - Application and OS Security - Database Security

High-Level Architecture - Security Components- Secure Single Sign-On- Public-Key Infrastructures- Firewalls- Intrusion Detection Systems-LDAP and X.500 Directories- Kerberos-Distributed Computing Environment-The Secure Shell, or SSH-The Distributed Sandbox- Security and Other Architectural Goals- Metrics for Non-Functional Goals-Force Diagrams around Security-High Availability- Robustness- Reconstruction of Events- Ease of Use- Maintainability, Adaptability, and Evolution- Scalability- Interoperability- Performance- Portability

MODULE– III **15**

Enterprise Security Architecture - Security as a Process-Security Data- Enterprise Security as a Data Management Problem- Tools for Data Management- David Isenberg and the “Stupid Network”-Extensible Markup Language- The XML Security Services Signaling Layer-XML and Security Standards- The Security Pattern Catalog Revisited-XML-Enabled Security Data-HGP: A Case Study in Data Management. Business Cases and Security: Building Business Cases for Security

TOTAL: 45

REFERENCE BOOKS

1. Jay Ramachandran, *“*Designing Security Architecture Solutions*”*, Wiley Computer Publishing, 2010.
2. Markus Schumacher, *“*Security Patterns: Integrating Security and Systems Engineering*”,* Wiley Software Pattern Series, 2010.

11MI017 VIDEO ANALYTICS

3 0 0 3

Objectives:

On completion of the course the students are expected

- To know the fundamental concepts of big data and analytics.
- To know various techniques for mining data streams.
- To acquire the knowledge of extracting information from surveillance videos.
- To know Event Modeling for different applications.
- To understand the models used for recognition of objects in videos

MODULE – I **15**

Introduction to big data & data analysis: Introduction to Big Data Platform – Challenges of Conventional systems – Web data – Evolution of Analytic scalability – analytic processes and tools – Analysis Vs Reporting – Modern data analytic tools – Data Analysis : Regression Modeling – Bayesian Modeling – Rule induction

Mining data streams: Introduction to Stream concepts – Stream data model and architecture – Stream Computing - Sampling data in a Stream – Filtering Streams – Counting distinct elements in a Stream – Estimating moments – Counting oneness in a window – Decaying window – Real time Analytics platform (RTAP) applications – case studies

MODULE - II **15**

Video analytics: Introduction – Video Basics – Fundamentals for Video Surveillance – Scene Artifacts Object Detection and Tracking: Adaptive Background Modeling and Subtraction – Pedestrian Detection and Tracking – Vehicle Detection and Tracking – Articulated Human Motion Tracking in Low – Dimensional Latent Spaces

Behavioral analysis & activity recognition: Event Modeling – Behavioral Analysis – Human Activity Recognition – Complex Activity Recognition – Activity Modelling using 3D shape, Video summarization, shape based activity models – Suspicious Activity Detection

MODULE- III **15**

Human face recognition & gait analysis: Introduction – Overview of Recognition algorithms – Human Recognition using Face – Face Recognition from still images – Face Recognition from video – Evaluation of Face Recognition Technologies – Human Recognition using gait – HMM Framework for Gait Recognition – View Invariant Gait Recognition - Role of shape and Dynamics in Gait Recognition

TOTAL : 45

REFERENCE BOOKS

1. Michael Berthold, David J.Hand, Intelligent Data Analysis, Springer, 2007.
2. Anand Rajaraman and Jeffrey David Ullman, Mining of Massive Datasets, Cambridge University Press, 2012.
3. Yunqian Ma, Gang Qian, “Intelligent Video Surveillance: Systems and Technology”, CRC Press (Taylor and Francis Group), 2009.
4. Rama Chellappa, Amit K.Roy-Chowdhury, Kevin Zhou.S, “Recognition of Humans and their Activities using Video”, Morgan & Claypool Publishers, 2005.

11MI018 ETHICAL HACKING

3 0 0 3

Objectives:

On completion of the course the students are expected

- To understand the security permissions in the network.
- To explore various network attacks.

MODULE – I **15**

Casing the Establishment: What is foot printing- Internet Foot printing-Scanning-Enumeration - basic banner grabbing- Enumerating Common Network services- Case study- Network Security Monitoring

Securing Permission - Securing file and folder permission- Using the encrypting file system- Securing registry permissions- Securing service- Managing service permission. Default services in windows 2000 and windows XP - Unix - The Quest for Root, Remote Access vs Local access. Remote access. Local access. After hacking root

MODULE - II **15**

Dial-up, PBX, Voicemail, and VPN hacking: Preparing to dial up- War-Dialing. Brute-Force Scripting PBX hacking - Voice mail hacking. VPN hacking - Network Devices – Discovery, Autonomous System Lookup - Public Newsgroups - Service Detection. Network Vulnerability - Detecting Layer 2 Media

Wireless Hacking: Wireless Foot printing. Wireless Scanning and Enumeration. Gaining Access - Tools that exploiting WEP Weakness- Denial of Services Attacks, Firewalls- Firewalls landscape- Firewall Identification-Scanning Through firewalls- packet Filtering- Application Proxy Vulnerabilities - Denial of Service Attacks - Motivation of Dos Attackers, Types of DoS attacks- Generic Dos Attacks - Unix and Windows DoS

MODULE- III **15**

Remote Control Insecurities: Discovering Remote Control Software. Connection – Weakness VNC - Microsoft Terminal Server and Citrix ICA - Advanced Techniques Session Hijacking - Back Doors. –Trojans – Cryptography, Subverting the systems Environment - Social Engineering - Web Hacking - Web server hacking web application hacking - Hacking the internet User - Malicious Mobile code, SSL fraud, E-mail Hacking, IRC hacking, Global countermeasures to Internet User Hacking

TOTAL : 45

REFERENCE BOOKS

1. Stuart McClure, Joel Scambray and Goerge Kurtz, “Hacking Exposed Network Security Secrets & Solutions”, Tata Mcgrawhill Publishers, 2010.
2. Bensmith, and Brian Komer, “Microsoft Windows Security Resource Kit”, Prentice Hall of India, 2010.

11MI019 GAME THEORY

3 0 0 3

Objectives:

On completion of the course the students are expected

- To know various algorithms in game theory.
- To deploy solutions for sequential games.

MODULE – I 15

Fundamentals: Conflict, Strategy and Games, Game theory, The Prisoner's Dilemma, Scientific metaphor, Business case, Games in normal and extensive forms – Representation, Examination, Examples

Non Cooperative Equilibria in Normal Games: Dominant Strategies and Social Dilemmas, Nash Equilibrium, Classical Cases in Game theory, Three person games, Introduction to Probability and Game theory, N-Person games

MODULE - II 15

Cooperative Solutions: Elements of Cooperative Games- Credible commitment, A Real Estate Development, Solution Set, Some Political Coalitions, Applications of the Core to Economics – The Market Game, The Core of a Two Person Exchange Game, The Core with More than Two Pairs of Traders, The core of Public Goods Contribution Game, Monopoly and Regulation

Sequential Games: Strategic Investment to Deter Entry, The Spanish Rebellion, Again, Imbedded Games – Planning Doctoral Study, Centipede Solved, Repeated play- Campers Dilemma, Pressing the shirts, Indefinitely Repeated Play – A Repeated Effort Dilemma, The Discount Factor

MODULE- III 15

Applications: Voting Games, Games and Experiments, Auctions, Evolution and Boundary Rational Learning - Case studies of Wireless Networks and Applications

TOTAL : 45

REFERENCE BOOKS

1. Roger A. McCain, "Game Theory – A Non-Technical Introduction to the Analysis of Strategy", Thomson South-Western, 2005.
2. Tirole, "Game Theory", MIT press 2005.
3. Osborne, "An Introduction to Game Theory", Oxford Press 2006.
4. E. N. Barron, "Game Theory: An Introduction", Wiley India Pvt Ltd, 2009.

11MI020 BIOMETRIC SECURITY

3 0 0 3

Objective:

On completion of the course the students are expected

- To analyze various biometric techniques.
- To adopt data mining techniques for behavioral biometrics.

MODULE – I **15**

Biometrics: Introduction- benefits of biometrics over traditional authentication systems –benefits of biometrics in identification systems-selecting a biometric for a system –Applications – Key biometric terms and processes - biometric matching methods -Accuracy in biometric systems

Physiological Biometric Technologies: Fingerprints - Technical description – characteristics - Competing technologies - strengths – weaknesses – deployment - Facial scan – Technical description - characteristics - weaknesses-deployment - Iris scan - Technical description – characteristics - strengths – weaknesses – deployment - Retina vascular pattern – Technical description – characteristics - strengths – weaknesses – deployment - Hand scan – Technical description-characteristics - strengths – weaknesses deployment – DNA biometrics

MODULE - II **15**

Behavioral Biometric Technologies: Handprint Biometrics - DNA Biometrics - signature and handwriting technology - Technical description – classification - keyboard / keystroke dynamics - Voice – data acquisition - feature extraction - characteristics - strengths – weaknesses-deployment

MODULE - III **15**

Multi Biometrics: Multi biometrics and multi factor biometrics - two-factor authentication with passwords - tickets and tokens – executive decision - implementation plan-Case studies on Physiological, Behavioral and multifactor biometrics in identification systems.

TOTAL : 45

REFERENCE BOOKS

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi, “Biometrics -Identity verification in a network”, Wiley Eastern, 2002.
2. John Chirillo and Scott Blaul,” Implementing Biometric Security”, Wiley Eastern Publications, 2005.
3. John Berger,” Biometrics for Network Security”, Prentice Hall, 2004.

11MI021 UNIX INTERNALS

3 0 0 3

Objectives:

On completion of the course the students are expected

- To know basic concepts of UNIX Operating system.
- To recognize various issues in process management.
- To know about various memory management policies.

MODULE – I **15**

General Overview of the System: History – System structure – User perspective – Operating system services – Assumptions about hardware, Introduction to the Kernel : Architecture of the UNIX operating system – Introduction to system concepts - The Buffer Cache: Buffer headers – Structure of the buffer pool – Scenarios for retrieval of a buffer – Reading and writing disk blocks – Advantages and disadvantages of the buffer cache

Internal Representation of Files: Inodes – Structure of a regular file – Directories – Conversion of a path name to an Inode – Super block – Inode assignment to a new file – Allocation of disk blocks

MODULE - II **15**

System Calls for the File System: Open – Read – Write – File and record locking – Adjusting the position of file I/O – Lseek – Close – File creation – Creation of special files – Changing directory, root, owner, mode – stat and fstat – Pipes – Dup – Mounting and unmounting file systems – link – unlink

Processes: Process states and transitions – Layout of system memory – The context of a process – Saving the context of a process – Manipulation of the process address space – Sleep - Process Control: Process creation – Signals – Process termination – Awaiting process termination – Invoking other programs – user id of a process – Changing the size of a process - Shell – System boot and the INIT process – Process Scheduling.

MODULE - III **15**

Memory management policies: Swapping – Demand paging. The I/O Subsystem: Driver Interface – Disk Drivers – Terminal Drivers– Streams – Inter process communication

TOTAL : 45

REFERENCE BOOKS

1. Maurice J. Bach, “The Design of the Unix Operating System”, First Edition, Pearson Education, 1999.
2. B. Goodheart, J. Cox, “The Magic Garden Explained”, Prentice Hall of India, 1986.
3. S. J. Leffler, M. K. Mckusick, M. J. .Karels and J. S. Quarterman., “The Design and Implementation of the 4.3 BSD Unix Operating System”, Addison Wesley, 1998.

11MI022 SECURE CLOUD COMPUTING

3 0 0 3

Objectives:

On completion of the course the students are expected

- To know the fundamentals of cloud computing
- To understand the performance of Amazon cloud computing
- To understand the security features of cloud computing and disaster recovery

MODULE– I 15

Cloud Computing: The Cloud Versus Grid - Cloud Application Architectures - Cloud Computing components - Cloud Infrastructure Models - An Overview of Amazon Web Services

Amazon Cloud Computing: Amazon S3 - Amazon EC2 - Before the Move into the Cloud - The Shift to a Cloud Cost Model - Service Levels for Cloud Applications - Security –Disaster Recovery

MODULE– II 15

Design In Web And Database: Ready for the Cloud - Web Application Design - Machine Image Design - Privacy Design - Database Management

Disaster Recovery: Disaster Recovery Planning - Disasters in the Cloud - Disaster Management, Scaling a Cloud Infrastructure - Capacity Planning - Cloud Scale

MODULE– III 15

Security In Cloud: Network Security - Host Security - Compromise Response – Infrastructure security- Data Security and storage – Identity and access management – Security management in the cloud – Privacy – Audit and Compliance – Examples of a cloud service providers – Security as a cloud service - The Impact of Cloud Computing on the Role of Corporate IT – Future of the cloud

TOTAL: 45

REFERENCE BOOKS

1. George Reese, “Cloud Application Architectures: Building Applications and Infrastructure in the Cloud -Theory in Practice”, O’Reilly Publications, 2008
2. David S. Linthicum, “ Cloud computing and SOA Convergence in Your Enterprise”, Pearson Publications, 2010
3. George Reese, “Cloud Application Architectures, building Applications and Infrastructure in the Cloud”, O’Reilly Publications, 2011
4. Siani Pearson, “Privacy and Security for Cloud Computing”, Springer Publisher, 2012

11MS014 XML AND WEB SERVICES

(Common to M.E. Computer and Communication and Computer Science and Engineering)

3 0 0 3

Objectives:

On completion of the course the students are expected

- To understand the basics of XML, XML syntax, namespaces, grammars and document presentation
- To understand web service specifications for XML, XML Schema, SOAP, WSDL and UDDI

MODULE – I **15**

XML, DTD, XPATH: Introducing XML- XML Fundamentals-Document Type Definitions-Namespaces -Internationalization - XML as a Document Format -XML on the web - XSL Transformations(XSLT) - XPATH - XLinks -XPointers- XInclude

MODULE - II **15**

XSL, CSS And Schema: Cascading Style Sheets (CSS) - XSL Formatting Objects (XSL-FO) - Resource Directory Description Language (RDDL) -XML as a Data Format - XML Schemas - Programming Models - Document Object Model (DOM) - Simple API for XML (SAX), JDOM, JAXB, SAX Vs DOM, Working with SAX.

MODULE - III **15**

Web Services: Architecture of web services, business motivations - Technical motivations, Services Oriented Architecture – Architecting Web Services, SOAP, basic SOAP syntax, SOAP messages, implementations, Overview of WSDL and UDDI.

TOTAL : 45

REFERENCE BOOKS

1. Elliotte Rusty Harold, W. Scott Means, “XML in a Nutshell”, Third Edition, O'Reilly Media, Inc., 2004
2. Schmelzer, Ron and Vandersypen, Travis, “XML and Web Services Unleashed”, Pearson education, New Delhi, 2002
3. Ramesh Nagappan, Robert Skoczylas and Rima Patel Sriganesh, "Developing Java Web Services", Wiley Publishing Inc., 2004.
4. Sandeep Chatterjee, and James Webber, "Developing Enterprise Web Services", Pearson Education, New Delhi, 2004.
5. McGovern, et al., "Java Web Services Architecture", Morgan Kaufmann Publishers, 2005.

11MI023 SECURITY THREATS

3 0 0 3

Objectives:

On completion of the course the students are expected

- To understand different network security threats.
- To deploy tools for security management.

MODULE – I **15**

Introduction: Security threats - Sources of security threats- Motives - Target Assets and vulnerabilities – Consequences of threats- E-mail threats - Web-threats - Intruders and Hackers, Insider threats, Cyber crimes

Network Threats: Active/ Passive – Interference – Interception – Impersonation – Worms –Virus – Spam's – Ad ware - Spy ware – Trojans and covert channels – Backdoors – Bots – IP Spoofing - ARP spoofing - Session Hijacking - Sabotage-Internal treats- Environmental threats -Threats to Server security

MODULE - II **15**

Security Threat Management: Risk Assessment - Forensic Analysis - Security threat correlation– Threat awareness - Vulnerability sources and assessment- Vulnerability assessment tools -Threat identification - Threat Analysis - Threat Modeling - Model for Information Security Planning.

Security Elements: Authorization and Authentication - types, policies and techniques – Security certification - Security monitoring and Auditing - Security Requirements Specifications -Security Policies and Procedures, Firewalls, IDS, Log Files, Honey Pots

MODULE- III **15**

Access Control: Trusted Computing and multilevel security - Security models, Trusted Systems, Software security issues, Physical and infrastructure security, Human factors – Security awareness, training , Email and Internet use policies.

TOTAL : 45

REFERENCE BOOKS

1. Joseph M Kizza, "Computer Network Security", Springer Verlag, 2005
2. Swiderski, Frank and Syndex, "Threat Modeling", Microsoft Press, 2004
3. William Stallings and Lawrie Brown, "Computer Security: Principles and Practice", Prentice Hall, 2008.
4. Thomas Calabres and Tom Calabrese, "Information Security Intelligence: Cryptographic Principles & Application", Thomson Delmar Learning, 2004.

11MI024 DEPENDABLE DISTRIBUTED SYSTEMS

3 0 0 3

Objectives:

On completion of the course the students are expected

- To know various fault tolerant techniques.
- To explore and solve issues in fault recovery.

MODULE – I 15

Dependability Concepts: Faults and Failures – Redundancy – Reliability – Availability – Safety – Security – Timeliness – Fault-classification – Fault-detection and location – Fault containment – Byzantine failures – Fault injection – Fault-tolerant techniques – Performability metrics

Fault-tolerance in real-time systems – Space-time tradeoff – Fault-tolerant techniques (N-version programming – Recovery block – Imprecise computation; (m,k)- deadline model) – Adaptive fault-tolerance – Fault detection and location in real-time systems. Security Engineering – Protocols – Hardware protection – Cryptography – Introduction – The Random Oracle model – Symmetric Crypto- primitives – modes of operations – Hash functions – Asymmetric crypto primitives

MODULE - II 15

Distributed Systems: Concurrency – fault tolerance and failure recovery – Naming. Multilevel Security – Security policy model – The Bell Lapadula security policy model – Examples of Multilevel secure system – Broader implementation of multilevel security system - Multilateral security – Introduction – Comparison of Chinese wall and the BMA model – Inference Control – The residual problem

Banking and bookkeeping – Introduction – How computers systems works – Wholesale payment system – Automatic teller Machine – Monitoring systems – Introduction – Prepayment meters – Taximeters, Tachographs and trunk speed limits - Nuclear Command and control – Introduction – The kennedy memorandum – unconditionally secure authentication codes – shared control security – tamper resistance and PAL – Treaty verification - Security printing and seals – Introduction – History – Security printing – packaging and seals – systemic vulnerability – evaluation methodology

MODULE – III 15

Bio Metrics: Introduction – Handwritten signature – face recognition – fingerprints – Iris codes – Voice recognition - Emission Security – Introduction – Technical Surveillance and countermeasures – Passive Attacks – Active Attacks

Electronic and Information warfare – Introduction – Basics – Communication system – Surveillance and target acquisition – IFF system – Directed Energy Weapon – Information Warfare - Telecom Security – Introduction – Phone Breaking – Mobile phones – Network attack and defense – Protecting E-commerce systems- E – policy – Management issues – systems evaluation and assurance

TOTAL : 45

REFERENCE BOOKS

1. Ross J Anderson and Ross Anderson, “Security Engineering: A guide to building dependable distributed systems”, Wiley, 2001.
2. David Powell, “A generic fault-Tolerant architecture for Real-Time Dependable Systems”, Springer, 2001.
3. Hassan B Diab and Albert Y. Zomaya, “Dependable computing systems: Paradigm, Performance issues and Applications”, Wiley series on Parallel and Distributed Computing, 2000.

11MI025 ACCESS CONTROL AND IDENTITY MANAGEMENT SYSTEM

3 0 0 3

Objectives:

On completion of the course the students are expected

- To identify and use access control techniques.
- To understand various identity and trust management policies.

MODULE – I **15**

Access Control : Introduction - Attenuation of privileges – Trust and Assurance – Confinement problem - Security design principles– Identity Management models – local –Network - federal – global web identity – XNS approach for global Web identity - Centralized enterprise level Identity Management

Elements of trust paradigms in computing – Third party approach to identity trust – Kerberos - Explicit third party authentication paradigm – PKI approach to trust establishment – Attribute certificates – Generalized web of trust models – Examples

MODULE - II **15**

Mandatory Access Control: Comparing information flow in BLP and BIBA models – Combining the BLP and BIBA models – Chinese wall problem

Discretionary access control and Access matrix model – definitions – Safety problem – The take grant protection model – Schematic protection model – SPM rules and operations – Attenuating – Applications

MODULE - III **15**

Role Based Access Control : Hierarchical Access Control - Mapping of a mandatory policy to RABC – Mapping discretionary control to RBAC – RBAC flow analysis – Separation of Duty in RBAC – RBAC consistency properties - The privileges perspective of separation of duties – Functional specification for RBAC .

TOTAL : 45

REFERENCE BOOKS

1. Messaoud Benantar, "Access Control Systems, Security, Identity Management and Trust Models", Springer Publications, 2006.
2. Messoud Benantar, "Access Control Systems: Security, Identity Management and Trust Models", Springer, 2009.
3. Elena Ferrari and M. Tamer A-zsu , "Access Control In Data Management Systems", Morgan & Claypool Publishers, 2010.

11MI026 OBJECT ORIENTED SOFTWARE ENGINEERING

3 0 0 3

Objectives:

On completion of the course the students are expected

- To know how to identify objects, relationships, services and attributes through UML.
- To know various Object oriented designs

MODULE – I **15**

Introduction : System Concepts – Software Engineering Concepts – Development Activities – Managing Software Development – Unified Modeling Language – Overview –modeling concepts – deeper view into UML - Project Organization – Communication

Analysis : Requirements Elicitation – Concepts – Activities – Management – Arena Case Study - Analysis Object Model – Analysis – Concepts – activities - Managing analysis - CaseStudy

MODULE - II **15**

System Design: Decomposing the system – Overview of System Design – System Design Concepts – System Design Activities – Addressing Design Goals – Managing System Design –Case Study

Object Design and Implementation Issues : Reusing Pattern Solutions – Concepts – Activities – Managing Reuse – Case Study - Specifying Interfaces – Concepts – Activities –Management – Case Study - Mapping Models to Code – Concepts – Activities – Management –Case Study – Testing – Concepts – Activities – Management

MODULE - III **15**

Managing Change: Rationale Management – Concepts – Activities – Management -Configuration Management – Concepts – Activities – Management - Project Management -Concepts – Activities – Management – Software Life Cycle

TOTAL : 45

REFERENCE BOOKS

1. Bernd Bruegge and Alan H Dutoit, “Object-Oriented Software Engineering”, 2nd Edition, Pearson Education, 2010.
2. Timothy Lethbridge and Robert Laganiere, “Object-oriented Software Engineering: Practical Software Development using UML and Java”, Mc Graw Hill Publication, 2010.

11MI027 ADHOC AND WIRELESS SENSOR NETWORKS

3 0 0 3

Objectives:

On completion of the course the students are expected

- To understand the basics of networking sensors and various IEEE standard
- To explore the knowledge in infrastructure establishment and sensor network database
- To understand the concepts of sensor network platforms and tools

MODULE – I **15**

Ad Hoc Wireless Networks: Introduction, Issues, Ad hoc wireless Internet-MAC Protocols: Design issues, goals and classification, Contention Based Protocols: MACAW, FAMA, BTMA-Contention based protocols with reservation mechanism: DPRMA, FPRP, RTMAC - Contention based protocols with scheduling mechanisms: DPS, DWOP, DLPS, Protocols using directional antennas: MAC protocols using directional antennas, DBTMA, DMAC

Routing and Multicast Routing Protocols: Design issues and classification, Table-driven Routing protocols: DSDV, WRP, CGSR- On-demand routing protocols: DSR, AODV, TORA, LAR, ABR-Hybrid routing protocols: CEDAR, ZRP- Routing protocols with efficient flooding mechanisms: OLSR- Hierarchical: FSR- power-aware routing protocols-Multicast Routing Protocols: Design issues and operation, Architecture reference model, classification, Tree-based: BEMRP, MZRP, MAODV - Mesh-based protocols: ODMRP, DCMP, FGMP

MODULE - II **15**

Introduction: Overview of sensor networks- Constraints and challenges – Advantages of sensor networks-Applications- Collaborative processing – Tracking scenario –Problem formulation – Distributed representation and interference of states – Tracking multiple objects – sensor models- Performance comparison and metrics

Networking Sensors: Key assumption - Medium access control – S-MAC protocol – IEEE 802.15.4 standard and ZigBee - General Issues - Geographic, Energy -Aware Routing - Attribute based routing

MODULE- III **15**

Infrastructure Establishment: Topology control – Clustering -Time Synchronization – Localization and Localization services-Sensor tasking and control-Task driven sensing – Role of sensor nodes – Information based tasking - Routing and aggregation-Sensor Database Challenges – Querying the physical environment – Interfaces-High level database organization- In-network aggregation – Data centric storage – Data indices and range queries – Distributed Hierarchical aggregation – Temporal data

Sensor Network Platforms and Tools: Sensor Node Hardware – Sensor network programming challenges – Node level software platforms – Operating system - TinyOS – Node level simulators – State centric programming –Applications and future directions

TOTAL : 45

REFERENCE BOOKS

1. Feng Zhao, Leonidas Guibas, “Wireless sensor networks- an information processing approach”, Mogan Kanufmann publishers, 2004
2. C. Sivaram Moorthy, B.S Manoj, “Ad Hoc Wireless Networks: Architectures and Protocols”, Prentice Hall, 2004
3. Toh C.K., “AdHoc Mobile Wireless Networks: Protocols and Systems”, Prentice Hall PTR, 2001.
4. Perkins Charles E., “AdHoc Networking”, Addison – Wesley, 2000
5. Stefano Basagni, Marco Conti, Silvia Giordano and Ivan Stojmenovic, “Mobile AdHoc Networking”, Wiley – IEEE press, 2004.

11MI028 CYBER PHYSICAL SYSTEMS

3 0 0 3

Objectives:

On completion of the course the students are expected

- To know the applications of Cyber physical systems
- To understand the design of embedded systems suitable for Cyber physical systems

MODULE – I **15**

Introduction: Applications – motivating example – the design process-Modeling dynamic behaviors: newtonian mechanics – actor models – properties of systems – feedback control-Discrete dynamics: discrete systems – the notion of state – finite-state machines – extended state machines – non determinism – behaviors and traces

Hybrid Systems: modal models – classes of hybrid systems-Composition of state machines: concurrent composition – hierarchical state machines-Concurrent models of computation: structure of models – synchronous-reactive models – dataflow models of computation – timed models of computation

MODULE - II **15**

Design of Embedded Systems: Embedded processors: types of processors – parallelism-Memory architectures: memory technologies – memory hierarchy – memory models-Input and output: i/o hardware – sequential software in a concurrent world – the analog digital interface

Multi Tasking: Imperative programs – threads – processes and message processing- Scheduling : basics of scheduling – rate monotonic scheduling – earliest deadline first – scheduling and mutual exclusion – multiprocessor scheduling

MODULE- III **15**

Analysis and Verification: Invariants and temporal logic: invariants – linear temporal logic-Equivalence and refinement: models as specifications – type equivalence and refinement – language equivalence and containment – simulation – bisimulation- Reachability analysis and model checking: open and closed systems – reachability analysis – abstraction in model checking – model checking liveness properties

Quantitative Analysis: Problems of internet – programs as graphs – factors determining execution time – basics of execution time analysis – other quantitative analysis problems- Sets and functions: sets – relations and functions – sequences-Complexity and computability: effectiveness and complexity of algorithms – problems, algorithms and programs – turing machines and undecidability – intractability: P and NP

TOTAL : 45

REFERENCE BOOKS

1. Lee E.A and Seshia S.A , “Introduction to Embedded Systems - A Cyber-Physical Systems Approach”, First Edition , UC Berkeley, 2013
2. Peter Marwedel, “Embedded System Design – Embedded Systems Foundations of Cyber-Physical Systems”, Second Edition , Springer Publisher, 2011
3. http://LeeSeshia.org