PG Program [M. Tech.] Curriculum Structure
W.e.f AY 2019-20 and Applicable for batches admitted from AY 2019-20 to 2022-23

List of Abbreviations

Abbreviation	Title	No of courses	Credits	% of Credits
PSMC	Program Specific Mathematics Course	1	4	5.9%
PSBC	Program Specific Bridge Course	1	3	4.4%
DEC	Department Elective Course	3	9	13.2%
MLC	Mandatory Learning Course	2	0	0%
PCC	Program Core Course	6	22	32.4%
LC	Laboratory Course	2	2	2.9%
IOC	Interdisciplinary Open Course	1	3	4.4%
LLC	Liberal Learning Course	1	1	1.5%
SLC	Self Learning Course	2	6	8.8%
SBC	Skill Based Course	2	18	26.5%

Semester I

Sr. No.	Course Type	Course Code	Course Name	Teaching Scheme			Credits
				L	T	P	
1.	PSMC	IS-19001	Probability, Statistics and Queuing Theory	3	1	--	4
2.	PSBC	IS-19002	Foundation of Cryptography	3	--	--	3
3.	DEC		**Department Elective -I**	3	--	--	3
		IS(DE)-19001	1. Embedded Systems				
		IS(DE)-19002	2. Advancement in Networking				
		IS(DE)-19003	3. Machine Learning				
		IS(DE)-19004	4. Business Analytics				
4.	MLC	ML-19011	Research Methodology and Intellectual Property Rights	2	--	--	--
5.	MLC	ML-19012	Effective Technical Communication	1	--	--	--
6.1	PCC	IS-19003	Advanced Operating System	3	--	--	3
6.2	PCC	IS-19004	Information Theory and Coding	3	--	--	3
6.3	PCC	IS-19005	Computer Systems Security	3	--	--	3
6.4	LC	IS-19006	Advanced Operating System – Laboratory	--	--	2	1
6.5	LC	IS-19007	Information Theory and Coding – Laboratory	--	--	2	1
6.6	LC	IS-19008	Computer Systems Security - Laboratory	--	--	2	1
			Total	**21**	**1**	**6**	**22**

Semester II

Sr. No.	Course Type	Course Code	Course Name	Teaching Scheme			Credits
				L	T	P	
1.	IOC		Data Structures	3	--	--	3
2.	DEC		**Department Elective –II**	3	--	--	3
		IS(DE)-19005	1. Advanced Database and Information Retrieval				
		IS(DE)-19006	2. Cloud Computing and Security				
		IS(DE)-19007	3. Blockchain Technology				
3.	DEC		**Department Elective –III**	3	--	--	3
		IS(DE)-19009	1. Web Security				
		IS(DE)-19010	2. Internet of Things				
4.	LLC	LL-19001	Liberal Learning Course	--	--	--	1
5.1	PCC	IS-19009	Network Security	3		--	3
5.2	PCC	IS-19010	Wireless and Mobile Security	3		--	3
5.3	PCC	IS-19011	Digital Forensics and Data Recovery	3		--	3
5.4	LC	IS-19012	Network Security - Laboratory	--		2	1
5.5	LC	IS-19013	Wireless and Mobile Security – Laboratory	--		2	1
5.6	LC	IS-19014	Digital Forensics and Data Recovery – Laboratory	--		2	1
			Total	**18**	**--**	**6**	**22**

***:** Department is going to offer **'Data Structures'** as IOC for students of other departments.

Semester-III

Sr. No.	Course Type	Course Code	Course Name	Teaching Scheme			Credits
				L	T	P	
1.	SBC	IS-19015	Dissertation Phase – I	--	--	12	6
2.	SLC	IS-19016	Massive Open Online Course –I	3	--	--	3
3.	SLC	IS-19017	Massive Open Online Course –II	3	--	--	3
			Total	**6**	**--**	**12**	**12**

Semester-IV

Sr. No.	Course Type	Course Code	Course Name	Teaching Scheme			Credits
				L	T	P	
1.	SBC	IS-19018	Dissertation Phase – II	--	--	24	12
			Total	**--**	**--**	**24**	**12**

[IS-19001] Probability, Statistics and Queuing Theory

Teaching Scheme	**Examination Scheme**
Lectures: 3 hrs/week	T1, T2 – 20 marks each
Tutorial: 1hr/week	End-Sem Exam – 60

Course Outcomes:

Students will be able to:

1. Solve various problems on probability, statistics and queuing theory.
2. Analyze the given probabilistic model of the problem.
3. Use the techniques studied in probability, statistics and queuing theory to solve problems in domains such as data mining, machine learning, network analysis.

Unit 1: Basic Probability Theory [2 Hrs]

Probability axioms, conditional probability, independence of events, Bayes' rule, Bernoulli trials

Unit 2: Random Variables and Expectation [10 Hrs]

Discrete random variables: Random variables and their event spaces, Probability Mass Function, Discrete Distributions such as Binomial, Poisson, Geometric etc., Indicator random variables
Continuous random variables: Distributions such as Exponential, Erlang, Gamma, Normal etc., Functions of a random variable.
Expectation: Moments, Expectation based on multiple random variables, Transform methods, Moments and Transforms of some distributions such as Binomial, Geometric, Poisson, Gamma, Normal.

Unit 3: Stochastic Processes [6 Hrs]

Introduction and classification of stochastic processes, Bernoulli process, Poisson process, Renewal processes.

Unit 4: Markov chains [8 Hrs]

Discrete-Time Markov chains: computation of n-step transition probabilities, state classification and limiting probabilities, distribution of time between time changes, M/G/1 queuing system
Continuous-Time Markov chains: Birth-Death process (M/M/1 and M/M/m queues), Non-birth-death processes, Petri nets.

Unit 5: Statistical Inference [8 Hrs]

Parameter Estimation – sampling from normal distribution, exponential distribution, estimation related to Markov chains, Hypothesis testing.

Unit 6: Regression and Analysis of Variance **[6 Hrs]**

Least square curve fitting, Linear and non-linear regression, Analysis of variance

Text Books:

1. Ronald Walpole, Probability and Statistics for Engineers and Scientists, Pearson, ISBN-13: 978-0321629111.

References:

1. Kishor Trivedi, Probability and Statistics with Reliability, Queuing, and Computer Science Applications, John Wiley and Sons, New York, 2001, ISBN number 0-471-33341-7

[IS-19002] Foundation of Cryptography

Teaching Scheme	**Examination Scheme**
Lectures: 3 hrs/week	End - Sem Exam -60 T1, T2 – 20 marks

Course Outcomes

By the end of this course, students should be able to

1. Understand modern concepts related to cryptography and cryptanalysis
2. Analyze and use methods for cryptography and reflect about limits and applicability of these methods
3. Reason about the details and design philosophy of modern symmetric and public key systems
4. Have a better appreciation of the uses and limitations of the various categories of cryptographic algorithms and understand that great care is needed in their selection and use
5. Reason that security is a systems problem, and that technical methods such as cryptography can only form part of the solution

Unit I: Introduction **[5 Hrs]**

Computer Security Concepts, OSI Security Architecture, Elements Of Information Security, Security Policy, Security Techniques, Operational Model Of Network Security, Security Services, Security Attacks, Security Mechanisms.

Unit II: Classical Encryption Techniques **[7 Hrs]**

Symmetric Cipher Model, Encryption Methods, Classical Encryption Techniques, Substitution Ciphers, Transposition Ciphers, one-time pad, Cryptanalysis

Unit III: Number Theory **[7 Hrs]**

Modular Arithmetic, Euclidean Algorithm, Prime Numbers, Relatively Prime Numbers, Primitive Roots, Fermat's Little Theorem, Euler Totient Function, Extended Euclidean Algorithm, Chinese Remainder Theorem, Discrete Logarithms, Index Calculus Algorithm.

Unit IV: Private-key Encryption [7 Hrs]

Block Ciphers, Stream Ciphers, Block Cipher Principles, Feistel Ciphers, Data Encryption Standard (DES), Triple DES, Block Cipher Operations, Advanced Encryption Standard (AES), RC5, International Data Encryption Algorithm (IDEA), Differential and Linear cryptanalysis, Weak Keys.

Unit V: Public-key cryptosystems [7 Hrs]

Public-Key Cryptography, Key Management, Key Distribution, RSA, Timing Attack, Diffie-Hellman Key Exchange, Elliptic Curve Arithmetic, Elliptic Curve Cryptography [ECC], Zero-Knowledge Proof.

Unit VI: Homomorphic Encryption [6 Hrs]

Introduction, Some Classical Homomorphic Encryption Systems: Goldwasser-Micali scheme, Benaloh's scheme, Naccache-Stern scheme, Okamoto-Uchiyama scheme, Applications and Properties of Homomorphic Encryption Schemes.

Text books:

1. V. K. Pachghare, "Cryptography and Information Security", PHI Learning 3rd edition
2. Jonathan Katz, Yehuda Lindell, "Introduction to Modern Cryptography", CRC press.

Reference books:

1. Oded Goldreich, "Foundations of Cryptography Basic Tools", Cambridge University Press.
2. Johannes Buchmann,"Introduction to Cryptography", Springer
3. Nigel Smart, "Cryptography: An Introduction", 3rd edition

IS(DE)-19001] Embedded Systems

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
T1, T2 – 20 marks each
End-Sem Exam – 60

Course Outcomes:

Students will be able to:

1. Explain Characteristics & Salient Features of Embedded Systems
2. Analyze Architecture & Recent Trends of Embedded Systems
3. Discuss PIC and ARM families
4. Understand general process of embedded system development and implement them.
5. Explain communication interface for wired and wireless protocols

6. Discuss hardware and software design methodologies for embedded systems

Unit I: Overview of Embedded Systems **[4 Hrs]**

Introduction, Definition, Characteristics & Salient Features, Classification, Application Areas, Overview of Embedded System Architecture & Recent Trends

Unit II: Hardware Architecture **[8 Hrs]**

Embedded Hardware based on Microprocessors, Microcontrollers & DSPs. Study of PIC Microcontrollers: PIC16C6X/7X Family & Applications. Study of ARM Family : ARM 7,9,10 &11: Overview & Architecture Comparison, Detailed Study of ARM7-TDMI including Core Architecture, ARM/Thumb State, On Chip Debug & Development Support, AMBA Bus, Applications.

Unit III: Communication Interface **[6 Hrs]**

Serial, Parallel, Wired Wireless Protocols Wired : CAN ,I2C,USB, FireWire Wireless : Blue Tooth , IrDA, IEEE802.11

Unit IV: Software Architecture **[6 Hrs]**

Concepts: Embedded OS, Real-Time Operating Systems (RTOS), Detailed Study of RT Linux ,Hand Held OS, Windows CE. & Development Tools.

Unit V: Embedded Systems for Automotive Sector **[6 Hrs]**

Electronic Control Units (ECU) for Engine Management, Antilock Braking System (ABS), Crusie Control, Design Challenges, Legislative Emission Norm, Interface Standards, Developmental Tools Navigation Systems : Global Positioning System (GPS):Detailed Study & Applications.

Unit VI: **[4 Hrs]**

Smart Cards: Classifications, Interfacing, Standards & Applications.
RFID Systems: Technology, RFID Tag ,RFID Reader, Application.

Unit VII: Case Studies **[6 Hrs]**

Embedded System for Mobile Applications, DSP Based Embedded System, Networked Embedded System & Digital Camera.

Text Books:

- K.V.K. Prasad, Embedded / Real Time Systems: Concepts, Design and Programming Black Book, Dreamtech Press, 2005.

References:

- Vahid F. and Givargies T., Embedded Systems Design, John Wiley X. Sons, 2002

- John B Peatman, Design with PIC Microcontrollers, Pearson Education, 1998
- Liu, Real-Time Systems, Pearson Education, 2000.
- Technical Manuals of ARM Processor Family available at ARM Website on Net

[IS(DE)-19002] Advancement in Networking

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
T1, T2 – 20 marks each,
End-Sem Exam – 60

Course Outcomes:
Students will be:
1. Capable of understand and implement various routing protocols
2. To have in depth knowledge of socket programming
3. Aware of issues in SAN, SDN and Open Stack Networking

Unit 1: **[06 Hrs]**
Routing Protocols: Distance Vector (RIP), Link State (OSPF), Multicast Routing Protocols: Intradomain and Interdomain, IP Version 6 (IPv6).

Unit 2: **[06 Hrs]**
Transport Layer Introduction: Services and port numbers, TCP, UDP, and SCTP.

Unit 3: **[07 Hrs]**
Sockets Introduction, Elementary TCP Sockets, IO Multiplexing, Socket Options, Elementary UDP Sockets, elementary SCTP Sockets.

Unit 4: **[07 Hrs]**
Advanced Sockets, Daemon Processes and the Inetd Superserver, Advanced IO Options, Non blocking I/O.

Unit 5: **[08 Hrs]**
Routing Sockets, Broadcasting, Multicasting, Advanced UDP Sockets, Raw Sockets, Out-of-Band Data, Signal Driven IO, IP Options, Data Link Access.

Unit 6: **[06 Hrs]**
Storage and Networking, Software Defined Networks, Open Stack Networking, Neutron.

TEXT BOOKS:

1. Computer Networks: A Systems Approach, 4e. Larry L. Peterson and Bruce S. Davie, Publisher: Morgan Kaufmann; 4 edition (March 22, 2007), ISBN-10: 0123705487, ISBN-13: 978-0123705488
2. UNIX® Network Programming Volume 1, Third Edition: The Sockets Networking API By W. Richard Stevens, Bill Fenner, Andrew M. Rudof , Publisher :Addison Wesley, ISBN : 0-13-141155-1
3. Tom Clark, Designing Storage Area Networks,A Practical Reference for Implementing Fibre Channel and IP SANs, Addison-Wesley Professional, 2nd Edition, 2003.
4. Marc Farley, Building Storage Networks , Tata McGraw Hill
5. Thomas D NAdeau and Ken Grey, Software Defined Networking, O'Reilly, 2013
6. SDN and NFV Simplified SDN and NFV Simplified Jim Doherty Copyright © 2016 Pearson Education, Inc. ISBN-13: 978-0-13-430640-7
7. Open Stack Cloud Computing Cookbook, 2nd Edition, Kevin Jackson , Cody Bunch, Packt Publishing, 978-1-78216-758-7

[IS(DE)-19003] Machine Learning

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
T1, T2 – 20 marks each,
End-Sem Exam – 60

Course Outcomes:

Students will be able to:

1. Understand kinds of data with pre processing required on that data.
2. Think of all possible evaluation measures and diagnoses required on kinds of data
3. Apply learning techniques like classification, decision tress, naive bayesian model, clustering, SVM, ANN, etc., to solve a real-life problem.
4. Demonstrate the ability to analyze different machine learning algorithms using evaluation measure.
5. Build an application using machine learning techniques.

Unit1: Introduction [04 Hrs]

Introduction to Machine Learning - What is machine learning, Applications of ML, Design Perspective and Issues in ML, Supervised, Unsupervised Learning with applications and issues.

Unit2: Data Forms , Input, Output and Pre-processing [06 Hrs]

Data Forms- Data, information, kinds of data
Input - Concepts: instances and attributes

Output - Knowledge Representation: vector space model, decision tree or instance based representation
Preprocessing - For Numeric kind of data, For text kind of data

Unit 3: Diagnostic and Evaluation [06 Hrs]

Diagnostics: Training/validating/testing procedures, diagnosing bias versus variance and vice versa, regularization, learning curves
Evaluation: Confusion metric, precision , recall, tradeoff between both, F-measure, accuracy

Unit4: Classification, Probabilistic classifier [08 Hrs]

Introduction to Classification, issues regarding classification, Classification : Hypothesis representation, decision boundary, cost function, gradient descent, regularization.
Probabilistic Classifier : Maximum likelihood Estimate, Naive Bayesian model, Case studies.

Unit 5: Decision Trees and Clustering [08 Hrs]

Decision Trees: Representation, hypothesis, issues in Decision Tree Learning, Pruning, Rule extraction from Tree, Learning rules from Data
Clustering: Unsupervised learning technique, k-means and k-mediods algorithm, choosing value of k, EM algorithm. Case studies.

Unit 6: Neural Network and Support Vector Machines [08 Hrs]

Artificial neural network (ANN) : non-linear hypothesis, NN representation, examples, multi-class classification using ANN.
Support Vector Machines Objective(optimization), hypothesis, SVM decision boundary, kernels : RBF and others. Case studies.

References:

1. Tom Mitchell, Machine Learning, McGraw-Hill, 1997
2. Jiawei Han, Jian Pei, Micheline Kamber, Data Mining –Concepts and Techniques,Elsevier, 09-Jun-2011.
3. Ethem Alpaydin, Introduction to Machine Learning, PHI, 2005
4. K.P. Soman, R. Longonathan and V. Vijay, Machine Learning with SVM and Other Kernel Methods, PHI-2009
5. Christopher M. Bishop, Pattern Recognition and Machine Learning, Springer 2006
6. R.O. Duda, P.E. Hart, D.G. Stork. Pattern Classification, John Wiley and Sons, Second edition 2000

[IS(DE)-19004] Business Analytics

Teaching Scheme:
Lectures: 3 Hrs/week

Examination Scheme:
T1 and T2: 20 Marks each
End-Sem Exam: 60 Marks

Course Outcomes:

Student will be able to:

1. Interpret the basic concepts of Business Analytics (BA)
2. Evaluate business problems and determine suitable analytical methods
3. Compare and contrast different BA techniques.
4. Describe how data can be interpreted beyond its basic analysis to tell a story relevant and meaningful to its organization, and how these stories can be utilized to gain competitive advantage through strategic application.
5. Design case studies on social media analytics.

Unit I: Fundamentals of Business Analytics [8 Hrs]

Learning Objectives; Business Analytics Basics, Evolution of Business Analytics, Scope of Business Analytics, Analytical Methods and Models, Problem Solving and Decision Making.

Unit II: Descriptive Analytics with Python [8 Hrs]

Populations and Samples in Python, Types of Measures, Measures of Location, Measures of Dispersion, Measures of Shape, Measure of Association between two variables, Measuring Variability, Visualizing and Exploring Data: Data Visualization using Tableau, R, and Python, Statistical Methods for Summarizing Data, Statistical Thinking in Business Decisions, Details of Data Modelling.

Unit III: Predictive Analytics [9 Hrs]

Predictive Modelling and Analysis: Logic-Driven Modelling, Data-Driven Modelling, Analysing Uncertainty and Model Assumptions, Model Analysis Using Risk Solver Platform, Linear Regression model, Least square method, Multiple regression model, Inference and regression, Categorical Independent variable, Modelling nonlinear relationships

The Scope of Data Mining, Data Exploration and Reduction, Classification, Classification Techniques, Association Rule Mining, Cause-and-Effect Modelling.

Unit IV: Prescriptive Analytics [7Hrs]

Building Linear Optimization Models, Implementing Linear Optimization Models, Solving Linear optimization models, Graphical optimization of Linear Optimization, Using Optimization models for prediction and insight.

Unit V: Making Decisions [8 Hrs]

Making Decisions with Uncertain Information, Decision Trees, The Value of Information, Utility and Decision Making, Case Study of Social Media Analysis.

Text Books:

1. James R. Evans, "Business Analytics: Methods, Models, and Decisions", Pearson 2012.

Reference Books:

2. Thomas H. Davenport, Jeanne G. Harris and Robert Morison, "Analytics at Work: Smarter Decisions, Better Results", Harvard Business Press, 2010
3. R. N. Prasad, Seema Acharya, "Fundamentals of Business Analytics", Wiley 2016.
4. Anil Maheshwari, "Data Analytics made accessible"Amazon Digital Publication, 2014
5. Evan Stubbs, "Delivering Business Analytics: Practical Guidelines for Best Practice", Wiley 2013.
6. Rachel Schutt, Cathy O'Neil, "Doing Data Science", O'REILLY, 2016.

[ ] MLC- Research Methodology and Intellectual Property Rights

Teaching Scheme	**Evaluation Scheme**
Lectures: 1 hr/week	**Continuous evaluation**
	Assignments/Presentation/Quiz/Test

Course Outcomes (COs):

Student will be able to

1. Understand research problem formulation and approaches of investigation of solutions for research problems
2. Learn ethical practices to be followed in research
3. Apply research methodology in case studies
4. Acquire skills required for presentation of research outcomes (report and technical paper writing, presentation etc.)
5. Infer that tomorrow's world will be ruled by ideas, concept, and creativity
6. Gather knowledge about Intellectual Property Rights which is important for students of engineering in particular as they are tomorrow's technocrats and creator of new technology
7. Discover how IPR is regarded as a source of national wealth and mark of an economic leadership in context of global market scenario
8. Study the national & International IP system
9. Summarize that it is an incentive for further research work and investment in R & D, leading to creation of new and better products and generation of economic and social benefits

Unit I: **[5 Hrs]**

Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem.

Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, necessary instrumentations.

Unit II: **[5 Hrs]**

Effective literature studies approaches, analysis

Use Design of Experiments /Taguchi Method to plan a set of experiments or simulations or build prototype

Analyze your results and draw conclusions or Build Prototype, Test and Redesign

Unit III: **[5 Hrs]**

Plagiarism, Research ethics

Effective technical writing, how to write report, Paper.

Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee

Unit IV: **[4 Hrs]**

Introduction to the concepts Property and Intellectual Property, Nature and Importance of Intellectual Property Rights, Objectives and Importance of understanding Intellectual Property Rights

Unit V: **[7 Hrs]**

Understanding the types of Intellectual Property Rights: -Patents-Indian Patent Office and its Administration, Administration of Patent System – Patenting under Indian Patent Act , Patent Rights and its Scope, Licensing and transfer of technology, Patent information and database. Provisional and Non Provisional Patent Application and Specification, Plant Patenting, Idea Patenting,

Integrated Circuits, Industrial Designs, Trademarks (Registered and unregistered trademarks), Copyrights, Traditional Knowledge, Geographical Indications, Trade Secrets, Case Studies

Unit VI: **[4 Hrs]**

New Developments in IPR, Process of Patenting and Development: technological research, innovation, patenting, development, International Scenario: WIPO, TRIPs, Patenting under PCT

Reference Books:

1. Aswani Kumar Bansal : Law of Trademarks in India
2. B L Wadehra : Law Relating to Patents, Trademarks, Copyright,
    a. Designs and Geographical Indications.
3. G.V.G Krishnamurthy : The Law of Trademarks, Copyright, Patents and
    a. Design.
4. Satyawrat Ponkse: The Management of Intellectual Property.
5. S K Roy Chaudhary & H K Saharay : The Law of Trademarks, Copyright, Patents
6. Intellectual Property Rights under WTO by T. Ramappa, S. Chand.

7. Manual of Patent Office Practice and Procedure
8. WIPO : WIPO Guide To Using Patent Information
9. Resisting Intellectual Property by Halbert ,Taylor & Francis
10. Industrial Design by Mayall, Mc Graw Hill
11. Product Design by Niebel, Mc Graw Hill
12. Introduction to Design by Asimov, Prentice Hall
13. Intellectual Property in New Technological Age by Robert P. Merges, Peter S. Menell, Mark A. Lemley

[ ] MLC-Effective Technical Communication

Teaching Scheme:
Lectures: 1hr / week

Evaluation Scheme:
100M: 4 Assignments (25M each)

Course Outcomes (COs):

Student will be able to

1. Produce effective dialogue for business related situations
2. Use listening, speaking, reading and writing skills for communication purposes and attempt tasks by using functional grammar and vocabulary effectively
3. Analyze critically different concepts / principles of communication skills
4. Demonstrate productive skills and have a knack for structured conversations
5. Appreciate, analyze, evaluate business reports and research papers

Unit I: Fundamentals of Communication **[4 Hrs]**

7 Cs of communication, common errors in English, enriching vocabulary, styles and registers

Unit II: Aural-Oral Communication **[4 Hrs]**

The art of listening, stress and intonation, group discussion, oral presentation skills

Unit III: Reading and Writing **[4 Hrs]**

Types of reading, effective writing, business correspondence, interpretation of technical reports and research papers

Reference Books

1. Raman Sharma, "Technical Communication", Oxford University Press.
2. Raymond Murphy "Essential English Grammar" (Elementary & Intermediate) Cambridge University Press.
3. Mark Hancock "English Pronunciation in Use" Cambridge University Press.
4. Shirley Taylor, "Model Business Letters, Emails and Other Business Documents" (seventh edition), Prentise Hall
5. Thomas Huckin, Leslie Olsen "Technical writing and Professional Communications for Non-native speakers of English", McGraw Hill.

[IS-19003] Advanced Operating Systems

Teaching Scheme:
Lectures: 2 Hrs/week

Examination Scheme:
T1 and T2: 20 Marks each
End-Sem Exam: 60 Marks

Course Outcomes:

Student will be able to

1. Identify and solve problems in distributed, multiprocessor and database operating systems.
2. Explain the architectural features and solutions for implementing various virtualization features in operating systems.
3. Solve synchronization problems involving distributed and virtualized environments.

Unit I: Distributed Operating Systems [8 Hrs]

System Architecture Types, Issues in Distributed Operating Systems: Naming,Scalability, Security, Client-Server Model, Process Synchronization, Global Knowledge,etc. RPC, Message Passing. Absence of Global Lock, Absence of Shared Memory,Lamports's Logical Clocks, Chandy Lamport's Algorithm, Termination Detection,Distributed Mutual Exclusion, Non Token Based Algorithms, Ricart AgarwalaAlgorithm, Lamport's Algorithm, Generalised Non-Toekn Based Algorithm,Comparative performance Analysis.

Unit II: Synchronization [7 Hrs]

Clock synchronization, Event ordering, Mutual exclusion, Deadlock, Election algorithms, Desirable features of good global scheduling algorithms, Task assignment approach, Load balancing approach, Load sharing approach, Process management: Process migration, Threads Distributed Deadlock Detection, Centralized/Distributed/Hierarchical control, Path Pushing Algorithm, Edge-Chasing Algorithm, Ho-Ramamoorthy Algorithms.

Unit III:Resource Management in Distributed Systems [6Hrs]

Distributed File Systems: Mounting, Caching, Bulk Data Transfer, Design Issues, CacheConsistency, Scalability, Log Structured File systems; Distributed Shared Memory:Central-Server Algorithm, Full-Replication Algorithm, etc. Coherence Protocols,Granularity, Page Replacement; Distributed Scheduling: Load, Classification, LoadBalancing and Load Sharing, Policies for Transfer, Selection, Location, Information,Stability, Load Balancing Algorithms, Load Sharing Case Studies

Unit IV: Fault Tolerance, Recovery, Protection and Security [6 Hrs]

Atomic Actions and Commit, Commit Protocols, Voting Protocols, Dynamic Voting, Classification of Failures, Backward and Forward Error Recovery, Synchronous/Asynchronous Checkpoints and Recovery, Recovery in Concurrent Systems, Access Matrix Model, Advanced Models of Protection, Cryptography

Unit V: Multiprocessor and Database Operating Systems [6Hrs]

Tightly and Loosely Coupled systems, Interconnect networks, Caching, Hypercubearchitectures, Threads, Process Synchronization in MP systems, Process Scheduling inMP systems, Requirements of Database OS Case Study of MP/ Database OS

Unit VI: Virtualisation [7Hrs]

Introduction; Simulation, Emulation, Para-Virtualization, Full virtualization; x86 Virtualization: privileged instructions, control sensitive instructions, Trap andEmulate, Binary translation, x86 hardware virtualization vmxon/vmxoff, vmentry, vmexit;, Intel VTd, VMCS, Shadow page tables, EPT/NPT, Hadoop-mapReduce Cluster and Programming Model

Text Books:

1. Sinha P. K., Distributed Operating Systems Concepts and Design, PHI, 1997.
2. Tanenbaum A. S., Distributed Operating Systems, Pearson Education India, 1995.
3. IA-32/64 Software Developers' Manual Volume 3A, 3B

Reference Books:

1. Intel Virtualization Technology, http://www.cs.columbia.edu/~cdall/candidacy/pdf/Uhlig2005.pdf
2. Understanding Full Virtualization, Paravirtualization and Hardware Assist https://www.vmware.com/files/pdf/VMware_paravirtualization.pdf

[IS-19004] Information Theory and Coding

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
T1, T2 – 20 marks each,
End-Sem Exam – 60

Course Outcomes:

Students will be able to:

1. Gain substantial knowledge of information and entropy, and their use in information theory,
2. Learn principles data compression
3. Understand techniques of design and performance evaluation of error correcting codes
4. Design and develop solutions for technical issues related to information coding
5. Get exposure to emerging topics in information theory, coding and compression.

Unit 1: Introduction to Information Theory **[08 Hrs]**

Introduction to Information Theory and Coding, Definition of Information Measure and Entropy, Information rate, Extension of An Information Source and Markov Source, Adjoint of an Information Source, Joint and Conditional Information Measure, Properties of Joint and Conditional Information Measures and A Morkov Source, Asymptotic Properties of Entropy and Problem Solving in Entropy.

Unit 2: Introduction to Coding **[08 Hrs]**

Classification of codes, Kraft-McMillan inequality, Source coding theorem, Shannon- Fano coding, Huffman coding, Extended Huffman coding, mutual information - Discrete memory less channels – BSC, BEC – Channel capacity, Shannon limit.

Unit 3: Data Compression **[07 Hrs]**

Adaptive Huffman Coding, Arithmetic Coding, LZW algorithm, Perceptual coding, Masking techniques, Psychoacoustic model, Channel Vocoder, Linear Predictive Coding, Video Compression and H.261.

Unit 4: Network Coding **[07 Hrs]**

The Buttery Network, Wireless and Satellite Communications, Source Separation, the Max-Flow Bound, Single-Source Linear Network Coding: Acyclic Networks

Unit 5: Error Control Coding: Block Codes **[06 Hrs]**

Definitions and Principles: Hamming weight, Hamming distance, Minimum distance decoding- Single parity codes, Hamming codes, Repetition codes - Linear block codes, Cyclic codes – Syndrome calculation, Encoder and decoder – CRC

Unit 6: Error Control Coding: Convolutional Codes **[06 Hrs]**

Convolutional codes – code tree, trellis, state diagram - Encoding – Decoding: Sequential search and Viterbi algorithm – Principle of Turbo coding.

Text books:

1. T. M. Cover and J. A. Thomas, “Elements of Information Theory”, John Wiley & Sons, second edition
2. Ranjan Bose, “Information Theory, Coding and Cryptography”, 2E, Tata-McGraw Hill, second edition
3. Muralidhar Kulkarni and K. S. Shivaprakasha, “Information Theory and Coding”, Wiley India Pvt Ltd
4. Raymond W. Yeung, "Information Theory and Network Coding", Springer, 2008, ISBN: 978-0-387-79234-7,978-0-387-79233-0,978-1-4419-4630-0.

Reference books/paper(s):

1. D.J.C. MacKay, "Information Theory, Inference, and Learning Algorithms", Cambridge University Press
2. C. E. Shannon, A Mathematical Theory of Communication, Bell Sys. Tech Journ, 1948. (available online)

Web Resources:

1. NPTEL Course (Information Theory and Coding – IIT, Bombay) : http://nptel.ac.in/syllabus/117101053/
2. MIT OpenCourseWare (Information Theory) : http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-441-information-theory-spring-2010/index.htm

[IS-19005] Computer Systems Security

Teaching Scheme	**Examination Scheme**
Lectures: 3 hrs/week	T1, T2 – 20 marks each, End-Sem Exam - 60

Course Outcomes:

1. Evaluate vulnerabilities in the computer systems
2. Learn basic practical security principles and contribute to computer systems and infrastructure
3. Apply methods for authentication, and access control,
4. Employ the security fundamentals to the management aspects of computer system security

Unit 1: Introduction and Access Control [07 Hrs]

Threats, Attacks, and Assets, Security Functional Requirements, Fundamental Security Design Principles, Attack Surfaces and Attack Trees, Computer Security Strategy, Access Control Principles, Subjects, Objects, and Access Rights, Discretionary Access Control, Role-Based and Attribute-Based Access Control, Identity, Credential, and Access Management, Trust Frameworks.

Unit 2: Database Security [05 Hrs]

The Need for Database Security, Database Management Systems, Relational Databases, SQL Injection Attacks, Database Access Control, Inference, Database Encryption.

Unit 3: Malicious Software [05 Hrs]

Types of Malware, Advanced Persistent Threat, Propagation—Infected Content—Viruses, Propagation—Vulnerability, Exploit—Worms, Propagation—Social Engineering—Spam E-Mail, Trojans, Payload—System Corruption, Payload—Attack Agent—Zombie, Bots, Payload—Information Theft—Keyloggers, Phishing, Spyware, Payload— Stealthing— Backdoors, Rootkits, Countermeasures.

Unit 4: Software Security **[07 Hrs]**

Software Security Issues, Handling Program Input, Writing Safe Program, Code, Interacting with the Operating System and Other Programs, Handling Program Output.

Unit 5: Operating System Security **[08 Hrs]**

Introduction to Operating System Security, System Security Planning, Operating Systems Hardening, Application Security, Security Maintenance, Linux/Unix Security, Windows Security, Virtualization Security

Unit 6: Trusted Computing and Multilevel Security **[08 Hrs]**

The Bell-LaPadula Model for Computer Security, Other Formal Models for Computer Security, The Concept of Trusted Systems, Application of Multilevel Security, Trusted Computing and the Trusted Platform Module, Common Criteria for Information Technology Security Evaluation, Assurance and Evaluation.

References:

1. William Stallings, Lawrie Brown Computer Security: Principles and Practice, 3rd Edition, Pearson, 2015
2. D. Gollmann, Computer Security, 3rd Edition, John Wiley & Sons, 2011
3. C. Pfleeger and S. L. Pfleeger, Security in Computing,4th Edition, PHI, 2006
4. Hossein Bidgoli, Handbook of Information Security: Threats, Vulnerabilities, Prevention, Detection and Management, Volume 3, John Wiely and Sons, 2006
5. Matt Bishop, Introduction to Computer Security. Pearson, 2004

[IS-19006] Advanced Operating Systems Laboratory

Teaching Scheme:
Lectures: 2 Hrs/week

Examination Scheme:
Continuous Assessment: 50 Marks each
End-Sem Exam: 50 Marks

Course Outcomes:

Student will be able to

1. Implement different distributed cocepts like RPC, RMI
2. Learn basics of MPI and its implementation
3. Demonstrate the need of virtualization

List of Assignment:

1. A program to execute RPC/ gRPC concept on different hosts

2. A program to execute RMI concept on different hosts
3. Message Passing Interface study and cluster setup on LAN
4. Case Study on Intel VT enable architecture
5. Hadoop-MapReduce cluster setup
6. Mini Project

Reference Book:

1. Coulouris George, Dollimore Jean, Kindberg Tim, Blair Gordon, Distributed Systems: Concepts and Design, Fifth Edition, Pearson, 2017.

[IS-19007] Information Theory and Coding Laboratory

Teaching Scheme	**Examination Scheme**
Lectures: 2 hrs/week	Term Work – 50

At the end of the course, the student should be able to:

1. Demonstrate information theories and the types of coding techniques
2. Compute the capacity of various types of channels
3. Develop the various coding algorithms
4. Use different open source tools for information theory and coding

List of Assignments:

1. Apply Encoding and Decoding techniques and demonstrate with a program
2. Calculation of Discrete Entropy for given probabilities
3. Implement a program for calculating entropy of parts of Message
4. Compute The Entropy of Message/Text
5. Implement Noiseless (No Noise) Binary Channel
6. Calculate Binary Symmetric Channel (BSC) Capacity
7. Implement and test Shannon- Fano Code Algorithm for given probabilities
8. Implement the Huffman- Coding Algorithm
9. To study error linear block code error control coding technique

[IS-19008] Computer Systems Security Laboratory

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
Term Work- 60

Course Outcomes:

1. Evaluate vulnerabilities in the computer systems
2. Learn basic practical security principles and contribute to computer systems and infrastructure
3. Apply methods for authentication, and access control,
4. Employ the security fundamentals to the management aspects of computer system security

Suggested List of Assignments:

1. Implementation and analysis of Access control using different techniques learned
2. Demonstration of SQL injection attack and its counter measures
3. Implementation of malware detection using any technique
4. Demonstration of buffer overflow attack and its counter measures
5. Download, install and configure the Kali Linux VMWare image, Add a few (test) users to the system. Demonstrate Pluggable Authentication Modules (PAM) in the Kali Linux system.
6. Download and setup Metasploitable6, which is an intentionally vulnerable Linux virtual machine. Exploit at least one buffer-overflow vulnerability and at least one other nontrivial vulnerability with Metasploit. For each of the attacks give a brief summary what actions you performed and which (additional) sources you have used to exploit the system. Of course, if you want to play more with Metasploit, feel free to keep exploiting more vulnerabilities

[IOC] Data Structures

Teaching Scheme:
Lectures: 3 Hrs/week

Examination Scheme:
T1 and T2: 20 Marks each
End-Sem Exam: 60 Marks

Course Outcomes:

At the end of the course, students will demonstrate the ability to:

1. Apply and implement advanced data structures, such as B-trees, multi-way trees, balanced trees, heaps, priority queues, to solve computational problems
2. Analyze the time and space complexity of advanced data structures and their supported operations
3. Compare the time and space tradeoff of different advanced data structures and their common operations

Unit I: **[6 Hrs]**

Review of Basic Concepts: Abstract data types, Data structures, Algorithms, Big Oh, Small Oh, Omega and Theta notations, Solving recurrence equations, Master theorems, Generating function techniques, Constructive induction.

Unit II: **[8 Hrs]**

Advanced Search Structures for Dictionary ADT: Splay trees, Amortized analysis, 2-3 trees, 2-3-4 trees, Red-black trees, Randomized structures, Skip lists, Treaps, Universal hash functions.

Unit III: **[6 Hrs]**

Advanced Structures for Priority Queues and Their Extensions: Binary Heap, Min Heap, Max Heap, Binomial heaps, Leftist heaps, Skewed heaps, Fibonacci heaps and its amortized analysis, Applications to minimum spanning tree algorithms.

Unit IV: **[6 Hrs]**

Data Structures for Partition ADT: Weighted union and path compression, Applications to finite state automata minimization, Code optimization.

Unit V: **[6 Hrs]**

Graph Algorithms: DFS, BFS, Biconnected components, Cut vertices, Matching, Network flow; Maximum-Flow / Minimum-Cut; Ford–Fulkerson algorithm, Augmenting Path

Unit VI: **[8 Hrs]**

Computational Geometry: Geometric data structures, Plane sweep paradigm, Concurrency, Java Threads, Critical Section Problem, Race Conditions, Re-entrant code, Synchronization; Multiple Readers/Writers Problem

Text Books:

- Introduction to Algorithms; 3rd Edition; by by Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein; Published by PHI Learning Pvt. Ltd. ; ISBN-13: 978-0262033848 ISBN-10: 0262033844
- Algorithms; 4th Edition; by Robert Sedgewick and Kevin Wayne; Pearson Education, ISBN-13: 978-0321573513

References:

- Algorithms; by S. Dasgupta, C.H. Papadimitriou, and U. V. Vazirani; Published by Mcgraw-Hill, 2006; ISBN-13: 978-0073523408 ISBN-10: 0073523402

- Algorithm Design; by J. Kleinberg and E. Tardos; Published by Addison-Wesley, 2006; ISBN-13: 978-0321295354 ISBN-10: 0321295358

[IS(DE)-19005] Advanced Database and Information Retrieval

Teaching Scheme:
Lectures: 3 Hrs/week

Examination Scheme:
T1 and T2: 20 Marks each
End-Sem Exam: 60 Marks

Course Outcomes:

Student will be able to

1. Understand foundation of RDBMS theory, internal functioning of a typical RDBMS
2. Design and implement algorithms for various relational operators such as join, group by etc.
3. Analyze and understand latest trends of RDBMS.
4. Understand and discuss current issues and research in searching and information retrieval
5. Understand and analyze Query Language and Operation with respect to IR.
6. Analyze evaluation techniques and understand indexing and searching in IR

Unit I: Transaction Processing [7 Hrs]

Serial and Serializable Schedules, Locking System: Two Phase Locking, Concurrency Control by Timestamps, Serializability and Recoverability, The Dirty-Data Problem, Managing Rollbacks Using Locking, Logical Logging, Recovery From Logical Logs, ARIES (Algorithm for Recovery and Isolation Exploiting Semantics).

Unit II: Query Processing and Optimization [7 Hrs]

Architecture of Query Execution Engines, Disk Access, Aggregation and Duplicate Removal, Sorting and Hashing, Binary Matching Operations (Join Algorithms), Execution of complex query plans, Nested Relations, Additional Techniques for performance improvement, Query Evaluation Techniques for Large Databases, Basic Query Optimization.

Unit III: Latest Trends in Databases [7 Hrs]

Study of Hadoop Distributed File System; HIVE - Data warehousing application built on top of Hadoop, MapReduce-It is a patented software framework introduced by Google in 2004 to support distributed computing on large data sets on clusters of computers; Dynamo – It is a highly available, proprietary key-value structured storage system or a distributed data store; Eventual Consistency Model for Distributed Systems.

Unit IV: IR Modeling [5 Hrs]

Data Retrieval Vs Information Retrieval, Goals and history of IR, The impact of the web on IR, The role of AI in IR, Applications of IR, Basic Models of IR: Boolean and vectorspace retrieval models, ranked retrieval, weighting, cosine similarity.

Unit V: Query Languages and Operations [6 Hrs]

Keyword-Based Querying, Pattern Matching, User Relevance Feedback, Automatic Local Analysis, Automatic Global Analysis.

Unit VI: Indexing, searching and Evaluation [6 Hrs]

Introduction, Inverted Files - Construction, Searching, Suffix trees and suffix arrays, Signature files, Boolean queries, Sequential searching, Pattern matching, Structural queries, Compression. Evaluation: Precision, Recall and Alternative Evaluation Methods.

Text Books:

- J. D. Ullman, "Database System: The Complete Book" , Pearson, 1st Edition, 2003.
- Korth Silberschatz and Sudarshan, "Database System Concepts", Tata McGraw Hill, 6th Edition, 2011.
- Richardo Baeza –Yates, Berthier Ribiero-Neto "Modern Information Retrieval " Addison –Wesley.
- Christopher D. Manning "Introduction to Information Retrieval" Cambridge University Press, 2008.

Reference Books:

- R. Elmasri, and S. Navathe, "Fundamentals of Database Systems", Benjamin Cummings, Pearson, 6th Edition, 2010
- C J Van Rijsbergen "Information Retrieval", An online book by C J Van Rijsbergen, University of Glasgow.
- C. Mohan, ARIES: A Transaction Recovery Method Supporting Fine-Granularity Locking and Partial Rollbacks Using Write-Ahead Logging, ACM Transactions on Database Systems, Vol. 17, No. 1, March, 1992, pp. 94–162.
- Jeffrey Dean and Sanjay Ghemawat, MapReduce: Simplified Data Processing on Large Clusters, Communications of the ACM, vol. 51, no. 1, pp. 107-113, 2008

[IS(DE)-19006] Cloud Computing and Security

Teaching Scheme:
Lectures: 6Hrs/week

Examination Scheme:
T1 and T2: 20 Marks each
End-Sem Exam: 60 Marks

Course Outcomes:

Student will be able to

1. Understand fundamentals of cloud computing architectures based on current standards, protocols, and best practices intended for delivering Cloud based enterprise IT services and business applications.
2. Identify the known threats, risks, vulnerabilities and privacy issues associated with Cloud based ITservices.
3. Understand the concepts and guiding principles for designing and implementing appropriate safeguards and countermeasures for Cloud based IT services.
4. Understandapproaches to designing cloud services that meets essential Cloud infrastructure characteristics - on - demand computing, shared resources, elasticity and measuring usage.
5. Understand the industry security standards, regulatory mandates, audit policies and compliance requirements for Cloud based infrastructures.

Unit I: Fundamentals of Cloud Computing and Architectural Characteristics [6Hrs]
what is Cloud computing, Architectural and Technological Influences of Cloud Computing, Cloud deployment models - Public, Private, Community and Hybrid models, Scope of Control - Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Cloud Computing Roles, Risks and Security Concerns.

Unit II: Security Design and Architecture for Cloud Computing [6Hrs]
Guiding Security design principles for Cloud Computing - Secure Isolation, Comprehensive data protection, End-to-end access control, Monitoring and auditing, Quick look at CSA, NIST and ENISA guidelines for Cloud Security, Common attack vectors and threats.

Unit III: Secure Isolation of Physical & Logical Infrastructure [6Hrs]
Isolation - Compute, Network and Storage, Common attack vectors and threats, Secure Isolation Strategies - Multitenancy, Virtualization strategies, Inter-tenant network segmentation strategies, Storage isolation strategies.

Unit IV: Data Protection for Cloud Infrastructure and Service [7Hrs]
Understand the Cloud based Information Life Cycle, Data protection for Confidentiality and Integrity, Common attack vectors and threats, Encryption, Data Redaction, Tokenization, Obfuscation, PKI and Key Management, Assuring data deletion, Data retention, deletion and archiving procedures for tenant data, Data Protection Strategies.

Unit V: Enforcing Access Control for Cloud Infrastructure based Services [7Hrs]
Understand the access control requirements for Cloud infrastructure, Common attack vectors and threats, Enforcing Access Control Strategies - Compute, Network and Storage - Authentication and Authorization, Roles-based Access Control, Multi-factorauthentication, Host, storage and network access control options, OS Hardening and minimization, securing remoteaccess,

Verified and measured boot, Firewalls, IDS, IPS and honeypots.

Unit VI: Monitoring, Auditing and Management [7Hrs]

Proactive activity monitoring, Incident Response, Monitoring for unauthorized access, malicious traffic, abuse of systemprivileges, intrusion detection, events and alerts, Auditing – Record generation, Reporting and Management, Tamper-proofing audit logs, Quality of Services, Secure Management - User management, Identity management, Security Information and Event Management.

Text Books:

- Vic (J.R.) Winkler, "Securing The Cloud: Cloud Computing Security Techniques and Tactics" (Syngress/Elsevier) - 978-1-59749-592-9.
- Thomas Erl, "Cloud Computing Design Patterns" (Prentice Hall) - 978-0133858563.

Reference Books:

- John R. Vacca, "Cloud Computing Security: Foundations and Challenges" 1st Edition.

[IS(DE)-19007] Block-chain Technology

Teaching Scheme:
Lectures: 6 Hrs/week

Examination Scheme:
T1 and T2: 20 Marks each
End-Sem Exam: 60 Marks

Course Outcomes:

Student will be able to

1 Understand what is blockchain and its need, real world problem(s) that blockchain is trying to solve.
2 Understand and describe how blockchain works.
3 Understand the underlying technology of transactions, blocks, proof-of-work, and consensus building.

4 Understand blockchain existence in the public domain (decentralized, distributed) yemaintain transparency, privacy, anonymity, security, immutability, history.

Unit I: Course Introduction [6 Hrs]

Course objectives and outcomes, History of centralized services, trusted third party for transactions, Making a case for a trustless system, Why blockchain, Decentralized transactions, No permission for transactions needed.

Unit II: History [6 Hrs]

How and when blockchain/bitcoin started, Milestones on the development of bitcoin, Criticism, ridicule and promise of bitcoin, Sharing economy, Internet of Value.

Unit III: Overview of blockchain technology [6 Hrs]

What is blockchain, Transactions, Blocks, Hashes, Consensus, Verify and confirm blocks.

Unit IV: Hashes and Transactions [7 Hrs]

Hash cryptography, Encryption vs hashing, Recording transactions, Digital signature, Verifying and confirming transactions

Unit V: Blocks and blockchain [7 Hrs]

Hash pointers, Blocks.

Unit VI: Consensus building [7 Hrs]

Distributed consensus, Byzantine generals problem, Proof of work, Writing to the blockchain

Text Books:

- Arvind Narayanan, "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction" Princeton University Press (July 19, 2016)

Reading Material:

- https://bitcoin.org/bitcoin.pdf.
- http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.
- http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.
- http://chimera.labs.oreilly.com/books/1234000001802/ch02.html.
- http://chimera.labs.oreilly.com/books/1234000001802/ch07.html#_introduction_2.

- http://chimera.labs.oreilly.com/books/1234000001802/ch08.html.

[IS(DE)-19009] Web Security

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
End-Sem Exam – 60 Marks
T1, T2 Exams– 20 Marks

Unit I: Introduction
The Evolution of Web Applications, Common Web Application Functions, Benefits of Web Applications, Web Application Security, Key Problem Factors in Web Security, The New Security Perimeter, The Future of Web Application Security, Core Defense Mechanisms: Handling User Access, Handling User Input, Handling Attackers

Unit II: Web Application Technologies
The HTTP Protocol, Web Functionality, Encoding Schemes, Mapping the Application, Enumerating Content and Functionality, Analyzing the Application

Unit III: Web Authentication
Authentication Technologies, Design Flaws in Authentication and Mechanisms, Implementation Flaws in Authentication, Securing Authentication

Unit IV: Session Management and Access Control
Weaknesses in Token Generation, Weaknesses in Session Token Handling, Securing Session Management, Access Controls: Common Vulnerabilities Attacking Access Controls

Unit V: Attacking Data Stores
Injecting into SQL, NoSQL, XPath and LDAP, Attacking Back-End Components: Injecting OS Commands, Manipulating File Paths, Injecting into XML Interpreters, Injecting into Back-end HTTP Requests, Injecting into Mail Services, Cross-Site Scripting: Varieties of XSS, Finding and Exploiting XSS Vulnerabilities, Preventing XSS Attacks

Unit VI: Attacking Web Application and Architecture
Tiered Architectures, Shared Hosting and Application Service Providers, Attacking the Application Server: Vulnerable Server Configuration, Vulnerable Server Software, Web Application Firewalls

Text books:

1. Dafydd Stuttard, Marcus Pinto "The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws", Second Edition,John Wiley & Sons, Inc.

2. Bryan Sullivan, Vincent Liu - Web Application Security, A Beginner's Guide-McGraw-Hill Osborne Media (2011)

Reference books:

1. Elisa Bertino, Lorenzo Martino, Federica Paci, Anna Squicciarini (auth.) - Security for Web services and service-oriented architectures-Springer-Verlag Berlin Heidelberg (2010)
2. Hadi Nahari, Ronald L. Krutz - Web Commerce Security_ Design and Development-Wiley (2011)

[IS(DE)-19010] Internet of Things

Teaching Scheme	**Examination Scheme**
Lectures: 3 hrs/week	T1, T2 – 20 marks each
	End-Sem Exam – 60

Course Outcomes:

1. Identify and design the new models for market strategic interaction
2. Analyze various protocols for IoT
3. Design a middleware for IoT
4. Analyze and design different models for network dynamics

Unit I: **[08 Hrs]**

Introduction to IoT: - Definition and Characteristics. Web of Things V/s Internet of Things: - Two pillars of the web, architecture standardization for WoT, Platform middleware for IoT, Unified multitier WoT architecture, WoT portals and Business Intelligence. M2M to IoT: M2M Communication, Trends in Information and Communication Technology, Implications for IoT, Barrier and Concern for IoT.

Unit II: **[08 Hrs]**

IoT Architecture: Building architecture , Main design principles and needed capabilities, An IoT architectural overview. IoT Reference Model: IoT domain model, Information model, Functional model, Communication Model, Security Model. IoT Reference Architecture: Deployment and Operational view.

Unit III: **[06 Hrs]**

M2M and IoT Technology Fundamentals: Gateway, Local and wide area networking, Managing IoT, Data consideration for M2M data, M2M and IoT analytics, Knowledge

Management. Recent Protocol for IoT: Power line Communication, IPv6 over Low Power WPAN, Routing protocol for low Power and lossy network RPL, ZigBee Smart energy 2.0, ESPI M2M architecture, MQ telemetry transport.

Unit IV: **[06 Hrs]**

OS Requirement of IoT Environment: RiOT, mbed, Contiki, typical componants of an OS for low end IoT devices. Recent Protocol for IoT: Power line Communication, IPv6 over Low Power WPAN, Routing protocol for low Power and lo ssy network RPL, ZigBee Smart energy 2.0, ESPI M2M architecture, MQ telemetry transport.

Unit V: **[06 Hrs]**

Security for IoT: Security Issues, Challenges, Spectrum of security consideration, privacy consideration, Interoperability Issues, Regularity, Legal and Right Issues, A policy based framework for security and Privacy in IOT

Unit VI **[06 Hrs]**

IoT Smart Application: Agriculture, Smart cities, Smart Energy and Smart Grid, Smart Mobility and Transport, Smart Homes, Smart Building and Infrastructure, Smart Health etc. Case Studies: Leading tools manufacturer transform operation with IoT (CISCO), Market Disputation and Improved Customer Relationship, Internal transformation for IoT business model Reshapes connected Industrial Vehicle.

TEXT BOOKS:

1. Internet of Things : Converging Technologies for smart Environments and Integrated Ecosystems, Dr. Ovidiu Vermesan, Dr. Peter Friess, River Publication.
2. From Machine to Machine to the Internet of Things: Introduction to a new Age of Intelligence, Jan Hollar, Vlasios Tsiasis Mulligan, Stefan Avesand, Stamis Karnouskos, David Boyle, 1st Edition, Academic Press 2014.

REFERENCES:

1. The Internet of Things: An Overview, Understanding the issues and Challenges of More Connected World, Internet Society October 2015.
2. Designing the Internet of Things, Adrian McEwen, Hakim Cassimally.
3. Architecting the Internet of Things, Dieter Uckelmann, Mark Harrison, Florian Michahelles, Springer 2011.
4. Case Study: PTC Transformational Case Study, PTC.com, 2015.
5. Case Study: IoT Transformation at Car estream, Carestream Case Study, PTC.com 2015.
6. Operating System for low end devices in IOT: Survey, Oliver Hahm, Emmanuel Baccelli, Hauke Petersen, Nicolas Tsiftes, Dec 2015, HAL -hal-01245551.

[IS-19009] Network Security

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
End-Sem Exam – 60 Marks
T1, T2 Exams– 20 Marks

Course Outcomes:

By the end of this course, students should be able to

1. Understand security issues related to networking vulnerabilities, firewalls, intrusion detection systems
2. Identify infrastructure components including devices, topologies, protocols, systems software, management and security
3. Design and develop solutions for technical issues related to networking and security problems.
4. Apply footprinting, scanning, enumeration and similar techniques to discover network and system vulnerabilities
5. Analyze performance and risk factors of enterprise network systems

Unit I: Introduction [7 Hrs]
Overview of security in networking, Vulnerabilities in TCP/IP model, Vulnerabilities at Application layer, Transport Layer, Internetwork Layer, Network Access Layer.

Unit II: Message Authentication [7 Hrs]
Basic concepts, Authentication Methods, Message Digest, Kerberos, X.509 Authentication Service.

Unit: III Digital Certificates and PKI [7 Hrs]
Introduction, Algorithms for Digital Signature, Digital Signature Standards Private- Key Management, The PKIX model, Public key Cryptography Standards (PKCS).

Unit IV: MAIL and IP Security [6 Hrs]
Introduction, Pretty Good Privacy (PGP), MIME, S/MIME, IP Security Architecture, IPsec, IPv4, IPv6, Authentication Header Protocol, Encapsulating Security Payload Protocol, VPN.

Unit V: Web Security [6 Hrs]
Introduction, Secure Socket Layer (SSL), Secure Electronic Transaction (SET) Transport Layer Security (TLS), Secure Hyper Text Transfer Protocol (SHTTP)

Unit VI: Firewalls and IDS [6 Hrs]
Introduction, Types of Firewall, Firewall Architectures, Trusted System, Access Control, Intrusion Detection systems, types of IDS, Intrusion Prevention Systems (IPS), Honeypots.

Text books:

1. V. K. Pachghare, "Cryptography and Information Security", PHI, Second Edition
2. William Stallings, "Cryptography and Network Security, Principles and Practices", Pearson Education, Third Edition
3. Charlie Kaufman, Radia Perlman and Mike speciner, "Network security, Private communication in a Public World".
4.

Reference books:

1. Christopher M. King, "Security architecture, design deployment and operations", Curtis patton and RSA Press.
2. Stephen Northcatt, Leny Zeltser, "INSIDE NETWORK Perimeter Security", Pearson Education Asia.
3. Robert Bragge, Mark Rhodes, Heith straggberg, "Network Security the Complete Reference", Tata McGraw Hill Publication.

Web Resources:

1. http://nptel.iitm.ac.in/courses/106105031/
2. http://www.cert.org/
3. http://www.howard.edu/csl/research_crypt.htm
4. http://www.cs.purdue.edu/homes/ninghui/courses/426_Fall10/lectures.html
5. http://www.cs.uwp.edu/staff/lincke/infosec/
6. http://www.cisa.umbc.edu/courses/cmsc/426/fall06/
7. http://www.cs.northwestern.edu/~ychen/classes/cs395-w05/lectures.html
8. http://www.cs.iit.edu/~cs549/cs549s07/lectures.htm

[IS-19010] Wireless and Mobile Security

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
T1, T2 – 20 marks each,
End-Sem Exam - 60

Course Outcomes:

1. Gain knowledge on security and privacy topics in wireless and mobile networking
2. Understand the security and privacy problems in the realm of wireless networks and mobile computing
3. Apply proactive and defensive measures to counter potential threats, attacks and intrusions

4. Analyze the various categories of threats, vulnerabilities, and countermeasures in the area of wireless and mobile networking
5. Design secured wireless and mobile networks that optimize accessibility whilst minimizing vulnerability to security risks
6. Research in the field of mobile and wireless security and privacy

Unit1: Introduction **[08 Hrs]**

Introduction to wireless networks security: Wired vs. wireless network security, Threat categories and the OSI model, Vulnerabilities, Countermeasures, Security architectures. IEEE 802.11 standard security issues: Authentication and authorization mechanisms, Confidentiality and Integrity, pre-RSNA protocols (WEP), RSNA (802.11i), Key management, Threat analysis and case studies. Mobile networks security.

Unit 2: Securing Wireless Networks **[06 Hrs]**

Overview of Wireless security, Scanning and Enumerating 802.11 Networks, Attacking, 802.11 Networks, Attacking WPA protected 802.11 Networks, Bluetooth Scanning and Reconnaissance, Bluetooth Eavesdropping, Attacking and Exploiting, Bluetooth, Zigbee Security, Zigbee Attacks.

Unit 3: Ad-hoc Network Security **[07 Hrs]**

Security in Ad Hoc Wireless Networks, Network Security Requirements, Issues, and Challenges in Security Provisioning, Network Security Attacks, Key Management in Adhoc Wireless Networks, Secure Routing in Adhoc Wireless Networks.

Unit 4: Mobile Security **[06 Hrs]**

Mobile system architectures, Overview of mobile cellular systems, GSM and UMTS, Security architecture & Attacks, Vulnerabilities in Cellular Services, Cellular Jamming, Attacks & Mitigation, Security in Cellular VoIP Services, Mobile application security.

Unit 5: Security in Mobile Platforms **[07 Hrs]**

Android vs. ioS security model, threat models, information tracking, rootkits, Threats in mobile applications, analyzer for mobile apps to discover security vulnerabilities, Viruses, spywares, and keyloggers and malware detection.

Unit 6: Mobile Commerce Security **[06 Hrs]**

Reputation and Trust, Intrusion Detection, Vulnerabilities, Analysis of Mobile commerce platform, secure authentication for mobile users, Mobile commerce security, payment methods, Mobile Coalition key evolving Digital Signature scheme for wireless mobile Networks

Text Book:

1. S. Kami Makki, Peter Reiher, Kia Makki, Niki Pissinou, Shamila Makki, “Mobile and Wireless Network Security and Privacy”, Springer, ISBN 978-0-387-71057-0, 09-Aug- 2007

2. Anurag Kumar, D. Manjunath, Joy Kuri "Wireless Networking" Morgan Kaufmann Publishers, First edition, 2009.

Reference Books:

1. C. Siva Ram Murthy, B.S. Manoj, "Adhoc Wireless Networks Architectures and Protocols", Prentice Hall, ISBN 9788131706885, 2007
2. Noureddine Boudriga, "Security of Mobile Communications", ISBN 9780849379413, 2010.
3. Kitsos, Paris; Zhang, Yan, "RFID Security Techniques, Protocols and System-On-Chip Design ", ISBN 978-0-387-76481-8, 2008.
4. Johny Cache, Joshua Wright and Vincent Liu," Hacking Wireless Exposed:Wireless Security Secrets & Solutions ", second edition, McGraw Hill, ISBN: 978-0-07-166662-6, 2010.

[IS-19011] Digital Forensics and Data Recovery

Teaching Scheme:
Lectures: 3 hrs/week

Examination Scheme
T1 and T2: 20 Marks each
End Sem Exam - 60 marks

Course Outcomes:

Student will be able to

1. Explain various computer forensic techniques/phases
2. Demonstrate the knowledge of forensic examination related to Microsoft Windows and Linux artifacts
3. Analyze different disk drives and file systems used in different operating systems
4. Apply various tools during real world forensic investigation

Unit 1: Introduction: [7 Hrs]
Overview of Computer Crime, Forensic investigation Process, Types of investigation, Digital Forensic Evidence, Anti-forensics, Computer Forensic Model, Maintaining Professional Conduct, preparing for investigation and conduction, Report Writing, Data recovery, Forensic tools: OSForensics, FTK, WinHex.

Unit 2: Digital Evidence Acquisition: [7 Hrs]
Functions, Categorization, Order of Volatility, Admissibility of Evidence**,** Acquisition and seizure of evidence, Chain of Custody, Storage formats, Image Capturing Process, Image Validation, Imaging tools: ProDiscover, Linux dd command.

Unit 3: MS Windows Forensics: [10 hrs]
Windows artifacts, Program Execution artifacts, Windows Registry, Structure, Registry Analysis Tools, Taskbar Jump Lists, Automatic Destination, Custom Destination, Jump List Extract tools:

Structured Storage Viewer, Windows Event Logging Service, Events Structure, Eventvwr Tool, Volume Shadow Copies, Analysis Tools, Windows Shell Bags, BagMRU keys, Prefetch Files, Windows Shortcut, UserAssist, IconCache.db, Amcache.hve, RunMRU, SRUDB.dat

Unit 4: Windows File Systems: **[10 Hrs]**

Clusters and Sectors, FAT File System, FAT Boot Sector, Interpretation using WinHex, FAT Directories, File Allocation Table, File Slack, New Technology File System (NTFS), Comparison to FAT, NTFSWalker tool, Partition Boot Sector, Boot Sector in WinHex, Master File Table (MFT), MFT File Attributes, Directory Files (Index Nodes), $INDEX_ROOT, NTFS Encrypting File System (EFS), Whole Disk Encryption, NTFS Compressed Files, File Deletion, Recovery Mechanisms.

Unit 5: Linux File System: **[10 Hrs]**

Examining Linux File Structures, Ext4, Superblocks, Directory entries, Inodes, Data blocks, Acquiring file system images using dd, dcfldd, Write blocking options, Mounting images, Leveraging The Sleuth Kit (TSK) and Autopsy, fsslat, mmls, Forensic data from /etc, /usr, /var, /dev, /proc, Timeline Analysis.

Unit 6: Email Forensics: **[4 Hrs]**

Email Structure, working, Email Protocols, Examining email messages, Email Server Examination, Tracing emails, Email Forensics Tools

References:

1. Bill Nelson Amelia Phillips Christopher Steuart, "Guide to Computer Forensics and Investigations", 4th Edition, Course Technology, Cengage Learning, ISBN-13: 978-1-435-49883
2. Brian Carrier, "File System Forensic Analysis", Pearson education, 1st Edition, ISBN-13:978-0321268174
3. E. Casey, Handbook of Digital Forensics and Investigation, Academic Press, 1st Edition,2010, ISBN-13: 978-0123742674
4. Dejey, Murugan, Cyber Forensics, Oxford Higher Education, 2018

[IS-19012] Network Security Lab

Teaching Scheme	**Examination Scheme**
Lectures: 2 hrs/week	Term Work– 50 Marks

Course Outcomes:

By the end of this course, students should be able to

1. Understand security issues related to networking vulnerabilities, firewalls, intrusion detection systems
2. Identify infrastructure components including devices, topologies, protocols, systems software, management and security
3. Design and develop solutions for technical issues related to networking and security problems.
4. Apply foot printing, scanning, enumeration and similar techniques to discover network and system vulnerabilities
5. Analyze performance and risk factors of enterprise network systems

Suggested List of Assignments:

1. Install, Configure and study a Intrusion detection system (IDS).
2. Implementation of different message digest/hashing techniques such as MD5, SHA
3. Implementation of email security using PGP(create yourself a 1024 bit PGP key. Use your name and email address for your key label. Use PGP to verify the signature on this assignment.)
4. Demonstrate the use of honey pots for the implementation of IDS
5. Use the OpenSSL commands to create a CA root certificate, a server certificate, and two or more client certificates
6. Write a client-server package for file transfer. The server will listen on some network port. When it accepts a connection, it immediately starts up SSL. The server verifies that the client's certificate came from the proper CA; that's the authentication used.

[IS-19013] Wireless and Mobile Security Lab

Teaching Scheme	**Examination Scheme**
Lectures: 3 hrs/week	T1, T2 – 20 marks each
	End-Sem Exam – 60

Course Outcomes:

1. Gain knowledge on security and privacy topics in wireless and mobile networking
2. Understand the security and privacy problems in the realm of wireless networks and mobile computing
3. Apply proactive and defensive measures to counter potential threats, attacks and intrusions
4. Analyze the various categories of threats, vulnerabilities, and countermeasures in the area of wireless and mobile networking
5. Design secured wireless and mobile networks that optimize accessibility whilst minimizing vulnerability to security risks
6. Research in the field of mobile and wireless security and privacy

Suggested list of assignments:

1. Set up and configuration of wireless access point
2. To implement mobile network using NS2
3. Demonstrate the different types of attacks on wireless network and counter measures for the same
4. Get Eclipse (or your IDE of choice) set up and running the 4.0.X Android emulator.
5. Get a sample program (can be an existing program or one you write yourself) running on the provided phone. Study the Android operating system, working of permission model and the risks associated with Android applications
6. Implement android malware detection using any one technique.