College of Engineering, Pune

(An Autonomous Institute of Govt. of Maharashtra, Permanently Affiliated to S.P. Pune University)

Department of Computer Engineering and Information Technology

Curriculum Structure & Detailed Syllabus (PG Program)

M.Tech. – Information Security

(Effective from: A.Y. 2019-20)

Program Education Objections (PEOs) of the program

1. To inculcate skills among students to identify, analyze, develop, and deploy information system-based solutions
2. To motivate students to take up higher studies/research in the field of Information Security
3. To build competency among students to become entrepreneurs in the domain of Cyber Security and Computer Forensics
4. To make students capable of dealing with legal, ethical, socio-economic, technological issues related with information security

Program Outcomes (POs)

The post-graduate students will demonstrate:

a. Adequate knowledge of fundamentals of Information Security
b. Ability to analyze a problem critically using scientific approach, relevant tools and techniques
c. Appropriate research skills for exploring a new problem and solving it in best possible way
d. Ability to work ethically and carry out the work with social responsibility
e. Ability of life-long and continuous self learning
f. Ability to carry out collaborative and multidisciplinary work in a professional environment
g. Ability to identify strengths and weaknesses and continuously strive to improve oneself

Correlation between the PEOs and the POs

PO / PEO	A	b	c	D	e	f	g
1	✓	✓	✓		✓	✓	
2	✓	✓	✓	✓	✓	✓	✓
3	✓	✓		✓	✓		✓
4	✓	✓		✓		✓	

Note: The cells filled in with ✓ indicate the fulfilment/correlation of the concerned PEO with the PO

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				
		IS(DE)-19008	4. Software Design Techniques and Security				
3.	DEC		**Department Elective –III**	3	--	--	3
		IS(DE)-19009	1. Web Security				
		IS(DE)-19010	2. Internet of Things				
		IS(DE)-19011	3. Vulnerability Assessment and Penetration Testing				
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 marks

Course Outcomes

Students will be able to:

1. Solve problems related to basic probability theory
2. Solve problems related to basic concepts and commonly used techniques of statistics
3. Model a given scenario using continuous and discrete distributions appropriately and estimate the required probability of a set of events
4. Apply theory of probability and statistics to solve problems in domains such as machine learning, data mining, computer networks etc.

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

Course Outcomes

Students will 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 1: 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 2: Classical Encryption Techniques **[7 Hrs]**

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

Unit 3: 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 4: 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 5: 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 6: 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. 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 marks

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 1: Overview of Embedded Systems **[4 Hrs]**

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

Unit 2: 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 3: Communication Interface **[6 Hrs]**

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

Unit 4: 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 5: 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 6: Smart Cards and RFID Systems **[4 Hrs]**

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

Unit 7: Case Studies **[6 Hrs]**

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

Text Books

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

Reference Books

1. Vahid F. and Givargies T., Embedded Systems Design, John Wiley X. Sons, 2002
2. John B Peatman, Design with PIC Microcontrollers, Pearson Education, 1998
3. Liu, Real-Time Systems, Pearson Education, 2000.
4. 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 marks

Course Outcomes

Students will be:

1. Demonstrate familiarity with the routing protocols
2. Able to do socket programming
3. Demonstrate familiarity with SAN
4. Demonstrate familiarity with SDN and Open Stack Networking

Unit 1: **[6 Hrs]**

Routing Protocols: Distance Vector (RIP), Link State (OSPF), Multicast Routing Protocols: Intradomain and Interdomain, IP Version 6 (IPv6).

Unit 2: **[6 Hrs]**

Transport Layer Introduction: Services and port numbers, TCP, UDP, and SCTP.

Unit 3: **[7 Hrs]**

Sockets Introduction, Elementary TCP Sockets, IO Multiplexing, Socket Options, Elementary UDP Sockets, elementary SCTP Sockets.

Unit 4: **[7 Hrs]**

Advanced Sockets, Daemon Processes and the Inetd Superserver, Advanced IO Options, Non blocking I/O.

Unit 5: **[8 Hrs]**

Routing Sockets, Broadcasting, Multicasting, Advanced UDP Sockets, Raw Sockets, Out-of-Band Data, Signal Driven IO, IP Options, Data Link Access.

Unit 6: **[6 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

Reference Books

1. Tom Clark, Designing Storage Area Networks,A Practical Reference for Implementing Fibre Channel and IP SANs, Addison-Wesley Professional, 2nd Edition, 2003.
2. Marc Farley, Building Storage Networks , Tata McGraw Hill
3. Thomas D NAdeau and Ken Grey, Software Defined Networking, O'Reilly, 2013
4. SDN and NFV Simplified SDN and NFV Simplified Jim Doherty Copyright © 2016 Pearson Education, Inc. ISBN-13: 978-0-13-430640-7
5. 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 marks

Course Outcomes

Students will be:

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.

Unit 1: Introduction **[4 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.

Unit 2: Data Forms , Input, Output and Pre-processing **[6 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 **[6 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

Unit 4: Classification, Probabilistic classifier **[8 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 **[8 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 **[8 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.

Text Books

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

Reference Books

1. K.P. Soman, R. Longonathan and V. Vijay, Machine Learning with SVM and Other Kernel Methods, PHI-2009
2. Christopher M. Bishop, Pattern Recognition and Machine Learning, Springer 2006
3. 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, T2 - 20 marks each
End-Sem Exam: 60 marks

Course Outcomes

Students 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 1: 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 2: 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 3: 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 4: Prescriptive Analytics **[7 Hrs]**

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 5: 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 Book

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

Reference Books

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

[IS-19003] Advanced Operating Systems

Teaching Scheme
Lectures: 2 Hrs/week

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

Course Outcomes

Students will be able to:

1. Demonstrate familiarity with synchronization related issues in distributed, multiprocessor and database operating systems and the methods to address those issues
2. Demonstrate familiarity with resource management related issues in distributed, multiprocessor and database operating systems and the methods to address those issues
3. Demonstrate familiarity with security and fault tolerance related issues in distributed, multiprocessor and database operating systems and the methods to address those issues

4. Explain the architectural features and solutions for implementing various virtualization features in operating systems.

Unit 1: 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 2: 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 3:Resource Management in Distributed Systems [6 Hrs]

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 4: 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 5: Multiprocessor and Database Operating Systems [6 Hrs]

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 6: Virtualisation [7 Hrs]

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 marks

Course Outcomes

Students will be:

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 [8 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 **[8 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 **[7 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 **[7 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 **[6 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 **[6 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
Lectures: 3 hrs/week

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

Course Outcomes
Students will be able to:

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 **[7 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 **[5 Hrs]**
The Need for Database Security, Database Management Systems, Relational Databases, SQL Injection Attacks, Database Access Control, Inference, Database Encryption.

Unit 3: Malicious Software **[5 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 **[7 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 **[8 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 **[8 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.

Text Book

1. William Stallings, Lawrie Brown Computer Security: Principles and Practice, 3rd Edition, Pearson, 2015

Reference Books

1. D. Gollmann, Computer Security, 3rd Edition, John Wiley & Sons, 2011
2. C. Pfleeger and S. L. Pfleeger, Security in Computing,4th Edition, PHI, 2006
3. Hossein Bidgoli, Handbook of Information Security: Threats, Vulnerabilities, Prevention, Detection and Management, Volume 3, John Wiely and Sons, 2006
4. 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

Students 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
4. Use distributed environment to solve a real life problem

Suggested List of Assignments

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
Lectures: 2 hrs/week

Examination Scheme
Term Work – 50 marks

Course Outcomes

Students will 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

Suggested 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
Practical: 2 hrs/week

Examination Scheme
Term Work- 50 marks

Course Outcomes

Students will be able to:

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, T2 - 20 marks each
End-Sem Exam: 60 marks

Course Outcomes

Students will be able to:

1. Demonstrate familiarity with advanced/specialized data structures such as B-trees, multi-way trees, balanced trees etc
2. Implement algorithms using the data strictures such as such as B-trees, multi-way trees, balanced trees, heaps, priority queues, to solve computational problems
3. Analyze the time and space complexity of advanced data structures and their supported operations
4. Justify use of a particular data structure/set of data structures to solve a given problem under given constraints/resources

Unit 1 **[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 2 **[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 3 **[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 4 **[6 Hrs]**

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

Unit 5 **[6 Hrs]**

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

Unit 6 **[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

1. Thomas H. Cormen et al., "Introduction to Algorithms"; 3rd Edition; PHI Learning Pvt. Ltd. ; ISBN-13: 978-0262033848 ISBN-10: 0262033844
2. Robert Sedgewick and Kevin Wayne, "Algorithms"; 4th Edition, Pearson Education, ISBN-13: 978-0321573513

Reference Books

1. S. Dasgupta, C.H. Papadimitriou, and U. V. Vazirani; "Algorithms", Mcgraw-Hill, 2006; ISBN-13: 978-0073523408 ISBN-10: 0073523402
2. J. Kleinberg and E. Tardos, "Algorithm Design"; 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, T2 - 20 marks each
End-Sem Exam: 60 marks

Course Outcomes:

Students 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 1: 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 2: 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 3: 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 4: 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 5: Query Languages and Operations **[6 Hrs]**

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

Unit 6: 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

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

Reference Books

1. R. Elmasri, and S. Navathe, "Fundamentals of Database Systems", Benjamin Cummings, Pearson, 6th Edition, 2010
2. C J Van Rijsbergen "Information Retrieval", An online book by C J Van Rijsbergen, University of Glasgow.
3. 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.
4. 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, T2 - 20 marks each
End-Sem Exam: 60 marks

Course Outcomes

Students 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 1: Fundamentals of Cloud Computing [6 Hrs]

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 2: Security Design and Architecture for Cloud Computing [6 Hrs]

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 3: Secure Isolation of Physical & Logical Infrastructure [6 Hrs]

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 4: Data Protection for Cloud Infrastructure and Service [7 Hrs]

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 5: Enforcing Access Control for Cloud Infrastructure based Services [7 Hrs]

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 6: Monitoring, Auditing and Management [7 Hrs]

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

1. Vic (J.R.) Winkler, “Securing The Cloud: Cloud Computing Security Techniques and Tactics” (Syngress/Elsevier) - 978-1-59749-592-9.

2. Thomas Erl, “Cloud Computing Design Patterns” (Prentice Hall) - 978-0133858563.

Reference Book

1. John R. Vacca, “Cloud Computing Security: Foundations and Challenges” 1st Edition.

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

Teaching Scheme:
Lectures: 3 Hrs/week

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

Course Outcomes

Students 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 1: 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 2: 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 3: Overview of blockchain technology **[6 Hrs]**

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

Unit 4: Hashes and Transactions **[7 Hrs]**

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

Unit 5: Blocks and blockchain **[7 Hrs]**

Hash pointers, Blocks.

Unit 6: Consensus building **[7 Hrs]**

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

Text Book

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

Reading Material

1. https://bitcoin.org/bitcoin.pdf.
2. http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.
3. http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.
4. http://chimera.labs.oreilly.com/books/1234000001802/ch02.html.
5. http://chimera.labs.oreilly.com/books/1234000001802/ch07.html#_introduction_2.
6. http://chimera.labs.oreilly.com/books/1234000001802/ch08.html.

[IS(DE)-19009] Web Security

Teaching Scheme
Lectures: 3 hrs/week

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

Course Outcomes

Students will be able to:

1. Sketch out the development of web application architecture leading to a more modular approach web application architecture
2. Outline a range of benefits and potential problems associated with a specific approach to web application architecture with respect to security issues
3. Apply current best practices for designing secure web application which is robust to known and unknown attacks
4. Apply modern tools which enable creating applications that apply the aforementioned design, performance, and security concepts

Unit 1: Introduction **[4 Hrs]**

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 2: Web Application Technologies **[8 Hrs]**

The HTTP Protocol, Web Functionality, Encoding Schemes, Mapping the Application, Enumerating Content and Functionality, Analyzing the Application

Unit 3: Web Authentication **[8 Hrs]**

Authentication Technologies, Design Flaws in Authentication and Mechanisms, Implementation Flaws in Authentication, Securing Authentication

Unit 4: Session Management and Access Control **[6 Hrs]**

Weaknesses in Token Generation, Weaknesses in Session Token Handling, Securing Session Management, Access Controls: Common Vulnerabilities Attacking Access Controls

Unit 5: Attacking Data Stores **[8 Hrs]**

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 6: Attacking Web Application and Architecture **[6 Hrs]**

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
Lectures: 3 hrs/week

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

Course Outcomes

Students will be able to:

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 1 **[8 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 2 **[8 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 3 **[6 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 4 **[6 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 5 **[6 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 6 **[6 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. Dr. Ovidiu Vermesan, Dr. Peter Friess, "Internet of Things: Converging Technologies for smart Environments and Integrated Ecosystems" , River Publication.
2. Jan Hollar, Vlasios Tsiasis Mulligan, Stefan Avesand, Stamis Karnouskos, David Boyle, "From Machine to Machine to the Internet of Things: Introduction to a new Age of Intelligence", 1st Edition, Academic Press 2014.

Reference Books

1. The Internet of Things: An Overview, Understanding the issues and Challenges of More Connected World, Internet Society October 2015.
2. Adrian McEwen, Hakim Cassimally, "Designing the Internet of Things"
3. Dieter Uckelmann, Mark Harrison, Florian Michahelles, "Architecting the Internet of Things", 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. Oliver Hahm, Emmanuel Baccelli, Hauke Petersen, Nicolas Tsiftes, "Operating System for low end devices in IOT: Survey" , Dec 2015, HAL -hal-01245551.

[IS(DE)-19011] Vulnerability Assessment and Penetration Testing

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

Course Outcomes

Upon completion of the course students should be able to:

1. Plan a vulnerability assessment and penetration test for a network.
2. Execute a penetration test using standard hacking tools in an ethical manner.
3. Report on the strengths and vulnerabilities of the tested network.
4. Identify legal and ethical issues related to vulnerability and penetration testing.
5. Demonstrate, document, report on, and provide a clear roadmap for remediation of exposed security issues

Unit 1: Fundamentals **[6 Hrs]**

Need for Vulnerability Assessment , Risk prevention , Compliance requirements, The life cycles of Vulnerability Assessment and Penetration Testing : scoping, information gathering, vulnerability scanning, false positive analysis, vulnerability exploitation (Penetration Testing), report generation

Unit 2: Information Gathering and Scanning **[8 Hrs]**

Scan prerequisites, Scan-based target system admin credentials, Direct connectivity without a firewall, Scanning window to be agreed upon, Backup of all systems including

data and configuration, Creating a scan policy as per target system OS and information, Configuring a scan policy to check for an organization's security policy compliance, Gathering information of target systems , Active and Passive information gathering, Social Engineering Attacks, Port scanning tools

Unit 3: Scan and Vulnerability Analysis **[8 Hrs]**

Scan Result analysis, Report interpretation, Hosts Summary (Executive), Vulnerabilities By Host, Vulnerabilities By Plugin, False positive analysis, Understanding an organizations' environment, Target-critical vulnerabilities, Port scanning tools, Vulnerability analysis: False positives, Risk severity Applicability analysis, Fix recommendations, Vulnerability Exploitation: Metasploit, Buffer overflow, Fuzzing, Advanced binary exploitation: Reverse engineering, Static code analysis

Unit 4: Vulnerability Management **[8 Hrs]**

Vulnerability Assessment reports, Stages of vulnerability management : Identify, Assess, Remediate, Report, Improve, Monitor, Vulnerability management tools : Nessus, report customization, report automation, audit policies, Compliance reporting, auditing infrastructure, Compliance check for different OS and databases

Unit 5: Introduction to Penetration Testing **[6 Hrs]**

Phases of Penetration Testing, methodologies (Black Box/White Box/Fuzz), penetration testing for Software (Operating system, services, application), Hardware, Network, Processes, End-user behaviour, tools used for penetration testing, Virtual box, Configuration, Reading: Sample PenTest Report, Sample test cases or scenarios

Unit 6: Case Studies and tools **[8 Hrs]**

Penetration Testing types : Social Engineering Test, Web Application Test, Physical Penetration Test, Network Services Test, Client-side Test, Tools: Nmap, Nessus, Metasploit, Wireshark, OpenSSL, Acunetix, Intruder

Text Books:

1. Patrick Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy", Publisher: Syngress (2011)
2. Himanshu Kumar, "Learning Nessus for Penetration Testing" Packt Publishing, Birmingham- Mumbai, 2014
3. Steve Manzuik, André Gold,Chris Gatford, "Network Security Assessment from Vulnerability to Patch", Syngress Publishing, Inc., 2007

Reference Books:

1. Vivek Ramachandran, Cameron Buchanan "Kali Linux Wireless Penetration Testing Beginner's Guide", 2015 Packt Publishing
2. Justin Clarke-Salt "SQL Injection Attacks and Defense" 1st Edition, Syngress Publication
3. Prakhar Prasad "Mastering Modern Web Penetration Testing", October 2016 Packt Publishing

4. Wolf Halton, Bo Weaver, "Kali Linux 2: Windows Penetration Testing", June 2016 Packt Publishing

[IS-19009] Network Security

Teaching Scheme
Lectures: 3 hrs/week

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

Course Outcomes
Students will 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 1: 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 2: Message Authentication **[7 Hrs]**
Basic concepts, Authentication Methods, Message Digest, Kerberos, X.509 Authentication Service.

Unit 3: 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 4: 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 5: Web Security **[6 Hrs]**
Introduction, Secure Socket Layer (SSL), Secure Electronic Transaction (SET) Transport Layer Security (TLS), Secure Hyper Text Transfer Protocol (SHTTP)

Unit 6: 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".

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 marks

Course Outcomes

Students will be able to:

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

Unit 1: Introduction **[8 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 **[6 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 **[7 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 **[6 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 **[7 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 **[6 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, T2 - 20 marks each
End Sem Exam - 60 marks

Course Outcomes

Students 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

Text Book

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

Reference Books

1. Brian Carrier, “File System Forensic Analysis”, Pearson education, 1st Edition, ISBN-13:978-0321268174
2. E. Casey, Handbook of Digital Forensics and Investigation, Academic Press, 1st Edition,2010, ISBN-13: 978-0123742674
3. Dejey, Murugan, Cyber Forensics, Oxford Higher Education, 2018

[IS-19012] Network Security Lab

Teaching Scheme
Lectures: 2 hrs/week

Examination Scheme
Term Work– 50 Marks

Course Outcomes

Students will 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**
Practical: 2 hrs/week	Term Work – 50 marks

Course Outcomes

Students will be able to:

1. Get 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.

[IS-19014] Digital Forensics and Data Recovery Lab

Teaching Scheme
Practical: 2 hrs/week

Examination Scheme
Term Work – 50 marks

Course Outcomes

Students will be able to:

1. Apply forensic analysis tools to recover significant evidence for identifying computer crime.
2. Develop ability as well-trained as next-generation computer crime investigators among students.
3. Analyze the concerns the acquisition and investigation of evidence from all devices capable of storing digital data and is often related to the prosecution of cybercrime and fraud.
4. Use the tools and techniques of digital forensics investigators.

Suggested list of assignments

1. Study of Computer Forensics and different tools used for forensic investigation
2. To Recover Deleted Files using Forensics Tools
3. Study the steps for hiding and extract any text file behind an image file/ Audio file using Command Prompt.
4. To Extract Exchangeable image file format (EXIF) Data from Image Files using Exifreader Software
5. To make the forensic image of the hard drive using EnCase Forensics.
6. To Restoring the Evidence Image using EnCase Forensics
7. To Collect Email Evidence in Victim PC
8. To Extracting Browser Artifacts
9. To View Last Activity of Your PC

10. Find Last Connected USB on your system (USB Forensics)
11. Comparison of two Files for forensics investigation by Compare IT software
12. Live Forensics Case Investigation using Autopsy
13. Developing a psychological profile of cyber offenders
14. Packet capture and protocol analysis
15. Use Benford's Law to analyze a data set (Excel file) of sales figures for Fraud Investigations

[IS-19015] Dissertation Phase – I

Teaching Scheme:
--- NA ---

Examination Scheme:
End-Sem Evaluation: 100 marks

Course Outcomes
Students will be able to:
1. Demonstrate how the available literature can be searched for gathering information about a problem/domain
2. Identify the current status of the technology/research in the selected domain and open problems in the selected domain that have relevance to societal / industrial needs
3. Apply software engineering principles related to requirements gathering and analysis
4. Evaluate different design techniques and methods to find out the best feasible solution under given constraints for the chosen problem for dissertation
5. Deliver/produce artifacts such as requirements specification, detailed design etc.

Guidelines
The dissertation is a yearlong activity, to be carried out and evaluated in two phases. The dissertation may be carried out in-house or in industry allotted through the department. The project topic and internal guide (faculty member of the department) are decided at the beginning of Phase-I.
Student is expected to complete the following activities in Phase-I:
1. Literature survey
2. Problem Definition
3. Motivation for study and Objectives
4. Preliminary design / feasibility / modular approaches

Deliverables
1. A report having following details: Abstract, Problem statement, Requirements specification, Literature survey, Proposed solution, High level design description, Plan for implementation and testing in Phase-II
2. A presentation that covers the major points covered in the report
3. A proof of concept (preferable but not mandatory)

Evaluation
Two independent assessments will be done:
1. Internal guide will evaluate his/her student for 40 marks

2. A panel of External Examiner(s) and two senior faculty of the department will evaluate the work for 60 marks

The marks obtained in these two assessments will be combined to get final evaluation out of 100 marks. The grading, like other courses, will be relative.

The evaluation will take place based on criteria such as literature survey and well defined project problem statement, proposed high level system design, concrete plan for implementation and result generation, presentation etc.

The panel (external examiner(s) and senior faculty) will provide a report about suggestions/changes to be incorporated during Stage-II.

[IS-19016] Massive Open Online Course – I

To be selected in consultation with the faculty advisor. Evaluation scheme will depend upon the instructor or host institute.

[IS-19017] Massive Open Online Course – II

To be selected in consultation with the faculty advisor. Evaluation scheme will depend upon the instructor or host institute.

[IS-19018] Dissertation Phase – II

Teaching Scheme:
--- NA ---

Examination Scheme:
Midterm Evaluation : 50 marks
End-Sem Evaluation: 50 marks

Course Outcomes

Students will be able to:

1. Apply project planning principles and techniques for effective and efficient project execution
2. Apply software engineering principles related to implementation and testing of software solutions
3. Demonstrate familiarity with the entire lifecycle of a software product/solution
4. Get proficiency in the language(s)/tool(s)/libraries/technology used in the dissertation work
5. Deliver/produce artifacts such as code, test plan, test results, research paper(s) based on the dissertation work etc.
6. Demonstrate presentation skills required to present the work done in various forms (technical report/paper/presentation) at various platforms (conferences/journals/defense of the dissertation etc)

Guidelines

Student is expected to complete the following activities in Phase-II:

1. Implementation of the proposed approach in the first stage

2. Testing and verification of the implemented solution
3. Writing of a report and presentation
4. Publish the work done at suitable conference/in a journal

Deliverables

1. Code (if the project is in-house)
2. Dissertation report that gives overview of the problem statement, literature survey, design, implementation details, testing strategy and results of testing
3. All the artifacts created throughout the duration of dissertation such as requirements specification, design, project plan, test cases etc
4. Presentation based on the dissertation report
5. Research Paper(s) based on the dissertation work

Evaluation

Evaluation will be done in two steps: mid-term evaluation and final evaluation.

3. Mid-term evaluation
   Evaluation will be done by the internal guide and a qualified external examiner
   The internal guide will evaluate his/her student for 20 marks.
   External Examiner will provide evaluation for 30 marks

   The assessment is done on the criteria such as concrete system design, implementation status and concrete plan for completion of remaining tasks, presentation etc.

   The purpose of mid-term evaluation is to check preparedness of students for the final evaluation. External examiner may give suggestions for changes/corrections to be incorporated before the final evaluation. If the work done till then may not lead to successful completion of the dissertation in the remaining time, student can be asked to take extension.

4. Final Evaluation
   Internal guide and one external examiner will carry out the final evaluation. The guide will provide evaluation for 20 marks and the external examiner for 30 marks.

   The assessment will be done based on the criteria such as quality of implementation,
   result analysis, project outcomes (publications, patent, copyright, contribution to open source community, participation in project competition etc.), quality of report, presentation etc.

The total assessment of phase-II work is for 100 marks (mid-term evaluation for 50 marks and final evaluation for 50 marks) and the grading, like other courses, will be relative.