COEP Technological University, Pune

School of Computation Sciences

Department of Computer Science and Engineering

M. Tech in Information Security

Curriculum Structure and Detailed Syllabus

w.e.f AY 2024-25

INDEX

Program Educational Objectives (PEOs)

PEO 1. To make students eligible to take up higher studies/research
PEO 2. To build competency among students to take up jobs that require technical expertise and problem solving ability
PEO 3. To in culcate readiness among students for self learning
PEO 4. To build competency among students in applying technology to solve real-life socio-economic problems

Program Outcomes (POs)

PO 1. Adequate knowledge of fundamentals of Information Security
PO 2. Ability to analyze a problem critically using scientific approach, relevant tools and techniques
PO 3. Appropriate research skills for exploring a new problem and solving it in best possible way
PO 4. Ability to work ethically and carry out the work with social responsibility
PO 5. Ability of life-long and continuous self learning
PO 6. Ability to carry out collaborative and multidisciplinary work in a professional environment
PO 7. Ability to identify strengths and weaknesses and continuously strive to improve oneself

List of Abbreviations

Abbreviation	Title	No of courses	Credits	% of Credits
PSMC	Program Specific Mathematics Course	1	4	5.88%
PSBC	Program Specific Bridge Course	1	3	4.41%
PCC	Program Core Course	6	18	26.47%
PEC	Program Specific Elective Course	3	9	13.24%
LC	Laboratory Course	5	5	7.35%
VSEC	Vocational and Skill Enhancement Course	2	18	26.47%
OE	Open Elective	1	3	4.41%
SLC	Self-Learning Course	2	6	8.82%
AEC	Ability Enhancement Course	1	1	1.47%
MLC	Mandatory Learning Course	2	--	--
CCA	Co-curricular and Extracurricular Activities	1	1	1.47%
	Total	**25**	**68**	**100%**

Semester I

Sr. No.	Course Type	Course Code	Course Name	Teaching Scheme				Credits
				L	T	P	S	
1	PSMC	<tbd>	Probability, Statistics and Queuing Theory	3	1	0	1	4
2	PSBC	<tbd>	Algorithms and Complexity Theory	3	0	0	1	3
3	PCC	<tbd>	Principles of Cryptography	3	0	0	1	3
4	PCC & LC	<tbd>	Computer System Security	3	0	2	1	4
5	PCC & LC	<tbd>	Information Theory and Coding	3	0	2	1	4
6	AEC	<tbd>	Mini Project/ Seminar	0	0	2	1	1
7	PEC	<tbd>	Program Specific Elective Course-I 1. Advancement in Networking 2. Machine Learning 3. Python For Cyber Security 4. Courses in association with industries	3	0	0	1	3
8	MLC	<tbd>	Research Methodology and Intellectual Property Rights	0	0	0	2	-
9	MLC	<tbd>	Effective Technical Communication Skills	0	0	0	1	-
Total Credits								**22**

Semester II

Sr. No.	Course Type	Course Code	Course Name	Teaching Scheme				Credits
				L	T	P	S	
1	OE	<tbd>	Open Elective	3	0	0	1	3
2	PCC & LC	<tbd>	Network Security	3	0	2	1	4
3	PCC & LC	<tbd>	Digital Forensics and Data Recovery	3	0	2	1	4
4	PCC &LC	<tbd>	Wireless and Mobile Security	3	0	2	1	4
5	PEC	<tbd>	Program Specific Elective –II 1. Blockchain Technology 2. Secure Software Systems 3. Cloud Computing and Security 4. Courses in association with industries	3	0	0	1	3
6	PEC	<tbd>	Program Specific Elective –III 1. Web Security 2. Internet of Things and Security 3. Vulnerability Assessment & Penetration Testing 4. Courses in association with industries	3	0	0	1	3
7	CCA	<tbd>	Liberal Learning Course	0	0	2	2	1
Total Credits								**22**

- The department offers “Data Structures” as Open Elective for students of other departments

- **Exit option to qualify for PG Diploma in Information Security :**
  - Eight weeks domain specific industrial internship in the month of June-July after successfully completing first year of the program

Semester III

Sr. No.	Course Type	Course Code	Course Name	Teaching Scheme				Credits
				L	T	P	S	
1	SLC	<tbd>	Massive Open Online Course –I	3	--	--	-	3
2	SLC	<tbd>	Massive Open Online Course –II	3	--	--	-	3
3	VSEC	<tbd>	Dissertation Phase – I	--	--	12	18	6
Total Credits								**12**

Semester IV

Sr. No.	Course Type	Course Code	Course Name	Teaching Scheme				Credits
				L	T	P	S	
1	VSEC	<tbd>	Dissertation Phase – II	--	--	24	12	12
Total Credits								**12**

Semester I

[PSMC] Probability, Statistics and Queuing Theory	
Teaching Scheme Lectures : 3 hrs/week Tutorial :1hr/week Self-Study : 1 hr/week	**Examination Scheme** Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

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

[PSBC] **Algorithms and Complexity Theory**

Teaching Scheme	**Examination Scheme**
Lectures : 3 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

Course Outcomes

Students will be able to:

1. Determine different time complexities of a given algorithm
2. Demonstrate various design techniques using typical algorithms
3. Develop algorithms using various design techniques for a given problem.
4. Formalize and abstract from a given computational task relevant computational problems, reduce problems and argue about complexity classes

Unit-I: Mathematical Foundation **[6 Hrs]**

Growth of functions – Asymptotic notation, Standard notation and common functions, Summations, solving recurrences.

Unit-II: Analysis of Algorithms **[8 Hrs]**

Necessity of time and space analysis of algorithms, Worst case analysis of common algorithms and operations on elementary data structures (e.g. Heapsort), Average case analysis of Quicksort, Amortized analysis.

Unit-III: Standard Design Techniques-I **[6 Hrs]**

Divide and Conquer, Greedy method.

Unit-IV: Standard Design Techniques-II **[8 Hrs]**

Dynamic programming, Graphs and Traversals.

Unit-V: Standard Design Techniques-III **[6 Hrs]**

Backtracking, Branch-and-bound.

Unit VI: Complexity Theory **[6 Hrs]**

Lower-bound arguments, Introduction to NP-Completeness, Reducibility (SAT, Independent Set, 3VC, Subset Su, Hamiltonian Circuit etc), Introduction to approximation algorithms

Text Books:

1. Thomas Cormen, Charles Leiserson, Ronald Rivest and Cliford Stein, "Introduction to Algorithms", PHI

Reference Books:

1. Horowitz and S. Sahni. "Fundamentals of Computer Algorithms", Galgotia, 1991

[PCC] **Principles of Cryptography**

Teaching Scheme	**Examination Scheme**
Lectures : 3 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 Marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60 Marks

Course Outcomes:

Students will be able to:

1. Describe the mathematical foundations that support cryptographic algorithms.
2. Explore fundamental concepts in cryptography, including secret-key encryption, public-key cryptography and other algorithms to provide security services.
3. Gain an understanding of modern cryptosystems, their associated algorithms, and cryptanalysis techniques.
4. Recognize critical challenges in information security management and determine the appropriate cryptosystem to design an effective security solution.

Unit 1: Classical Encryption Techniques **[8 Hrs]**

Classical Encryption Techniques: Symmetric Cipher Model, , Substitution and Transposition Techniques, Cryptanalysis and Brute-Force Attack.

Block Ciphers: Stream Ciphers and block Ciphers, Feistel Cipher structure, Data Encryption Standard (DES), Strength of DES, Block cipher design principles, Tripple DES, Modes of Operation

Unit 2: Public-Key Cryptography **[6 Hrs]**

Number Theory: Testing for Primality, Chinese Reminder Theorem, Discrete Logarithms

Public Key Cryptography: Principles of public-key cryptosystems

RSA: RSA algorithm, the security of RSA,ElGamal Cryptographic systems

Unit 3: Data Integrity Algorithms **[8 Hrs]**

Cryptographic Hash Functions: Message Authentication, security requirements of Hash functions, MD5

Message Authentication Code (MAC): requirements for Message Authentication Codes,

MACs Based on Hash Functions: HMAC, MACs Based on Block Ciphers: DAA and CMAC
Digital Signature: Elgamal Scheme, DSA (Digital Signature Algorithm), Elliptic Curve Digital Signature Algorithm (ECDSA), Digital Signature Standard (DSS), Security of Digital Signatures.

Unit 4: Key Management and User Authentication [6 Hrs]
Key Management and Distribution: Symmetric Key Distribution, Diffie-Hellman Key Agreement, Distribution of Public Keys, X-509 Certificates.
User Authentication: Remote user Authentication principles, Authentication using Symmetric encryption, Kerberos, Authentication using Asymmetric encryption, Federated Identity Management.

Unit 5: Modern Cryptosystems [8 Hrs]
Modern Symmetric Cipher:
Finite Fields: Groups, rings, fields, Modular Arithmetic, Polynomial Arithmetic, Euclid's algorithm, GF(p), $GF(2^p)$
Advanced Encryption Standard (AES), Evaluation Criteria
Elliptic Curve: Elliptic curve arithmetic, Elliptic curve cryptography, Analog of Diffie-Hellman key exchange, security of ECC.
Quantum Cryptography: Properties of Quantum States, One-time Pad, Quantum Key Distribution (QKD), BB84 Protocol, Security of QKD, Comparison with Classical Cryptography.

Unit 6: Technology for Secure Computation [4 Hrs]
Data Privacy, Searchable Encryption, Homomorphic Encryption,PHE, SHE, FHE, Verifiable Computation, Zero Knowledge Proofs, Multi-Party Computation, Functional Encryption

Topics for Self study [4 Hrs]
Matrix operations, Primality Testing, Steganography, RC4 stream cipher, Public Key Infrastructure, SHA-512.

Text Books:

1. William Stallings: Cryptography and Network Security, Pearson 7th edition, 2017
2. Atul Kahate, Cryptography and Network Security, McGraw-Hill, Fourth edition, 2019

References:

1. V K Pachghare: Cryptography and Information Security, PHI 2nd edition, 2015
2. Forouzan, Cryptography and Network Security, Tata McGraw-Hill, 2008
3. Mark A. Will, Ryan K. L. Ko, A Guide to Homomorphic Encryption, The Cloud Security Ecosystem, Elsevier, pp. 101–127, 2015
4. Anne Broadbent, Christian Schaffner, Quantum Cryptography Beyond Quantum Key Distribution, Designs, Codes and Cryptography. Volume 78, Issue 1, pp 351-382, 2016

[PCC & LC] Computer Systems Security

Teaching Scheme	**Examination Scheme**
Lectures : 3 hrs/week Labs: 2 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 Marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60 Marks Laboratory: CIE: 50 Marks, (Orals): 50 Marks

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 withthe 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, WindowsSecurity, 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 theTrusted 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

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

[PCC & LC] Information Theory and Coding

Teaching Scheme	**Examination Scheme**
Lectures : 3 hrs/week	Mid Sem. Exam (MSE) : 30 Marks
Labs: 2 hrs/week	Teachers Assessment (TA) : 10 Marks
Self-Study : 1 hr/week	End Sem. Exam (ESE) : 60 Marks
	Laboratory:
	CIE: 50 Marks, (Orals): 50 Marks

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, VideoCompression and H.261.

Unit 4: Network Coding [07 Hrs]

The Buttery Network, Wireless and Satellite Communications, Source Separation, the Max-FlowBound, 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”, WileyIndia 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.

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

[PEC] - Advancement in Networking

Teaching Scheme	**Examination Scheme**
Lectures : 3 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 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, ElementaryUDP 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 ImplementingFibre Channel and IP SANs, Addison-Wesley Professional, 2nd Edition, 2003.
4. Open Stack Cloud Computing Cookbook, 2nd Edition, Kevin Jackson , Cody Bunch, PacktPublishing, 978-1-78216-758-7

[PEC] Machine Learning

Teaching Scheme	Examination Scheme
Lectures : 3 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 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 evaluationmeasure.
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 dataInput - 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 viceversa, 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 : Hypothesisrepresentation, 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, Ruleextraction from Tree, Learning rules from Data

Clustering: Unsupervised learning technique, k-means and k-mediods algorithm, choosing valueof 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 KernelMethods, 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, Secondedition 2000

[PEC] Python for Cyber Security

Teaching Scheme	**Examination Scheme**
Lectures : 3 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

Course Outcomes:

Students will be able to:

1. Learn python basics and its features
2. Use object oriented programming
3. Use python advanced libraries.
4. Implement packet sniffers, port scanners using socket programming
5. Implement cybersecurity mechanism

Unit 1: Introduction to Python **[8 Hrs]**

Python Basics: Introduction, Why python? Installation of python, setting up the environment, Features of Python, Writing and executing Python program, real time applications of python

Python Syntax: Variables and Data Types, Operators, type casting, Input operation, Comments, Strings and operations on strings flow controls-if, if-else structures, for loop, while loop, break and continue statements, functions, lists and dictionaries

Unit 2: Object Oriented Programming **[8 Hrs]**

Concept of object-oriented programming, creating classes and objects in python, Parameterized and non-parameterized constructors in python, in-built class methods and attributes, Encapsulation, Polymorphism, Inheritance and its types, data abstractions.

Unit 3: Scripting tools and libraries **[8 Hrs]**

Importing and using modules, introduction to os module, ping script, pinging multiple targets,

File operations such as creating file, reading a file, writing to the file, Network security related libraries such as Beautiful Soup, YARA, Scapy, Cryptography, Requests, Pylibnet, pymetasploit3

Unit 4: Sockets **[8 Hrs]**

Sockets, Types of sockets, Socket programming using python, network port scanning, packet sniffing using python, TCP packet injection, discovering hidden vulneraries using pymetasploit3, checking SQL injections and cross site scripting, Geolocation Extraction, Real time extraction from social media

Unit 5: Cybersecurity **[8 Hrs]**

Environment requirement, the MITRE ATT&CK and Shield frameworks, Active scanning, search open technical databases, valid accounts, replication through removable media, boot or logon AutoStart execution, boot or logon initialization scripts, hijack execution flow, Impair defenses, hide artifacts,

Unit 6: Reconnaissance and accessing credentials **[8 Hrs]**

Performing reconnaissance on target environment, establishing command and control channels, collecting sensitive data such as user credentials on the system, defensive python for detection of suspicious connections, account discovery, file and directory discovery

Text Books:

1. Howard E. Potson: Python for Cybersecurity: Using Python for Cyber offense and Defense, John Wiley

2. Justin Seitz, Tim Arnold: Black Hat Python: Python programming for Hackers and Pentesters, 2nd Edition, no starch press

[MLC] Research Methodology and Intellectual Property

Teaching Scheme	**Examination Scheme**
Self-Study :2 hrs/week	Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

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

technicalpaper 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 studentsof 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 aneconomic 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 socialbenefits

Unit I: **[5 Hrs]**

Meaning of research problem, Sources of research problem, Criteria Characteristics of a goodresearch 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 simulationsor 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 bya 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 PropertyRights

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 , PatentRights 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	**Examination Scheme**
Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

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 andattempt 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 reportsand research papers

Reference Books

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

Reference books/paper(s):

1. D.J.C. MacKay, "Information Theory, Inference, and Learning Algorithms", CambridgeUniversity 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

Semester II

[OE] Data Structures	
Teaching Scheme Self-Study : 1 hr/week	**Examination Scheme** Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

Course Outcomes

Students will be able to:

1. Decide appropriate data structures such as B-trees, heaps etc that best suits for solving a real life problem
2. Implement advanced data structures, 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. 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:

1. 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
2. Algorithms; 4th Edition; by Robert Sedgewick and Kevin Wayne; Pearson Education, ISBN-13: 978-0321573513

References:

1. Algorithms; by S. Dasgupta, C.H. Papadimitriou, and U. V. Vazirani; Published by Mcgraw-Hill, 2006; ISBN-13: 978-0073523408 ISBN-10: 0073523402
2. Algorithm Design; by J. Kleinberg and E. Tardos; Published by Addison-Wesley, 2006; ISBN-13: 978-0321295354 ISBN-10: 0321295358

[PCC & LC] Network Security	
Teaching Scheme Lectures : 3 hrs/week Labs: 2 hrs/week Self-Study : 1 hr/week	**Examination Scheme** Mid Sem. Exam (MSE) : 30 Marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60 Marks Laboratory: CIE: 50 Marks, (Orals): 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

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 Firewalls, 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.

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.

[PCC & LC] Digital Forensics and Data Recovery	
Teaching Scheme Lectures : 3 hrs/week Labs: 2 hrs/week Self-Study : 1 hr/week	**Examination Scheme** Mid Sem. Exam (MSE) : 30 Marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60 Marks Laboratory: CIE: 50 Marks, (Orals): 50 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

[PCC & LC] Wireless and Mobile Security

Teaching Scheme	**Examination Scheme**
Lectures : 3 hrs/week Labs: 2 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 Marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60 Marks Laboratory: CIE: 50 Marks, (Orals): 50 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

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.

[PEC] - Block-chain Technology

Teaching Scheme	**Examination Scheme**
Lectures : 3 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

Course Outcomes:

Student will be able to

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

andconsensus 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: Histor [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 ComprehensiveIntroduction" 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.

[PEC] Secure Software Systems

Teaching Scheme	Examination Scheme
Lectures : 3 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

Course Outcomes:

Student will be able to

1. Evaluate a secure software development process including designing secure applications,writing secure code against attacks.
2. Assess the reports through security testing procedures
3. Solve the security issues of vulnerabilities, flaws, and threats.
4. Identify and use the standard Secure Coding Principles for design secure software systems
5. Develop secured web programming to enhance the software code more resistant to attacks.
6. Identify the need of Security and safety metrics

Unit I: Introduction [6 Hrs]

What is System engineering-Systems engineering and the systems-System engineering processes-Understanding Software systems engineering-The software system engineering processes-Steps inthe software development processes-Functional and non-functional requirements Verification andvalidation

Unit II: Engineering secure and safe systems [7 Hrs]

Introduction-The approach-security versus safety-Four approaches to develop critical systems- Thedependability approach-The safety engineering approach-The secure systems approach- The real-time systems approach Security-critical and safety-critical systems

Unit III:Architecting Secure Software Systems [7 Hrs]

Security Requirements Analysis, Threat Modelling, Security Design Patterns Anti-Patterns, Attack Patterns, Security Design Patterns, Authentication, Authorization -Security Coding Security Algorithm, Security Protocol, Key Generation

Unit IV: Validating Security [7 Hrs]

Generating the Executable, Security Testing vulnerability assessment, code coverage tools - Secured Deployment, Security Remediation, Security Documentation, Security ResponsePlanning, Safety-Critical Systems

Unit V: Security in web-facing applications [7 Hrs]

Overview of web security, Identity Management, publickey infrastructure, Code injection, Pa-rameter tampering, secured web programming, application vulnerability description language

Unit VI: Security and safety metrics [6 Hrs]

Defining metrics-differentiating measures and metrics Software Metrics-Measuring and re- porting metrics Metrics for meeting requirements-Risk metrics-Security

metrics for software systems-safetymetrics for software systems

Text Books:

1. Asoke K. Talukder, Manish Chaitanya, Architecting Secure Software Systems,ISBN 9781420087840, 2008
2. John Musa D, Software Reliability Engineering, 2nd Edition, Tata McGraw-Hill, 2005.

[PEC] Cloud Computing and Security

Teaching Scheme	**Examination Scheme**
Lectures : 3 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

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 Cloudbased 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 Characteristic [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 andTactics" (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.

[PEC] Web Security	
Teaching Scheme Lectures : 3 hrs/week Self-Study : 1 hr/week	**Examination Scheme** Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

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 andExploiting 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)

[PEC] Internet of Things Security

Teaching Scheme	**Examination Scheme**
Lectures : 3 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

Course Outcomes:

1. Identify and describe the variety of IoT systems architectures, essential components and challenges specific to IoT systems
2. Apply appropriate security mechanisms for IoT to real-world problems.
3. Reflect on the impact of current and future IoT technologies on security and privacy.
4. Interpret information privacy and data protection requirements in regards to IoT products design.

Unit I: **[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 II: **[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 III: **[6 Hrs]**

Security Classification and Access Control Data classification (Public and Private), Internet of Things Authentication and Authorization, Internet of Things Data Integrity

Unit IV: **[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 V: **[6 Hrs]**

Attacks and Implementation of Internet of Things Denial of Service, Sniffing, Phishing, DNS Hijacking, Pharming, Defacement, Firmware of the device, Web Application Dashboard , Mobile Application Used to Control, Configure and Monitor the Devices

Unit VI: **[6 Hrs]**

Security Protocols and Management Firmware of the device, Web Application Dashboard , Mobile Application Used to Control, Configure and Monitor the Devices, Identity and Access Management, Key Management

TEXT BOOKS:

1. Internet of Things : Converging Technologies for smart Environments and Integrated Ecosystems, Dr. Ovidiu Vermesan, Dr. Peter Friess, River Publication.
2. Practical Internet of Things Security. Packt Publishing Limited
3. Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations. CRC Press

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, FlorianMichahelles, Springer 2011.
4. Operating System for low end devices in IOT: Survey, Oliver Hahm, Emmanuel Baccelli,Hauke Petersen, Nicolas Tsiftes, Dec 2015, HAL -hal-01245551.
5. Hersent, O., Boswarthick, D., & Elloumi, O. (2015). The Internet of Things: Key Applications and Protocols. Wiley