COEP Technological University, Pune

School of Engineering and Technology

Department of Computer Science and Engineering

M. Tech in Computer Science and Information Security

Curriculum Structure and Detailed Syllabus

w.e.f AY 2025-26

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 inculcate 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)

The post-graduate students will demonstrate:

PO 1. An ability to independently carry out research /investigation and development work to solve practical problems
PO 2. An ability to write and present a substantial technical report/document
PO 3. Students should be able to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program
PO 4. Ability to manage/work in teams with diverse backgrounds in different aspects (such as language, region, technical proficiency, engineering discipline etc) and communicate effectively
PO 5. Ability to life-long self learning and to keep oneself up-to-date in the field of technology
PO 6. Understand intellectual property rights and the ability to apply them in an appropriate manner

List of Abbreviations

Abbreviation	Title	No of courses	Credits	% of Credits
PSMC	Program Specific Mathematics Course	1	4	5.00%
PSBC	Programme Specific Bridge Course	1	3	3.75%
PCC + LC	Programme Core Course + Laboratory Course	6	24	30.00%
PEC	Programme Elective Course	3	9	11.25%
OJT	On Job Training	1	3	3.75%
OE	Open Elective	1	3	3.75%
LLC	Liberal Learning Course	1	1	1.25%
SLC	Self Learning Course	2	6	7.50%
RM	Research Methodology	1	3	3.75%
AEC	Ability Enhancement Course	1	2	2.50%
Project	Project	2	22	27.5
	Total	20	80	100%

Curriculum Structure

Semester I

Sr. No.	Course Type	Course Code	Course Name	L	T	P	S	Cr	Evaluation Scheme (Weightages in %)				
									Theory			Laboratory	
									MSE	TA	ESE	ISE	ESE
1.	PSMC	<tbd>	Probability, Statistics and Queuing Theory	3	1	-	1	4	30	20	50	-	-
2.	PSBC	<tbd>	Algorithms and Complexity Theory	2	-	2	1	3	30	20	50	50	50
3.	PCC	<tbd>	Principles of Cryptography	3	-	2	1	4	30	20	50	50	50
4.	PCC	<tbd>	Computer System Security	3	-	2	1	4	30	20	50	50	50
5.	PCC	<tbd>	Information Theory & Coding	3	-	2	1	4	30	20	50	50	50
6.	PEC-1	<tbd>	Programme Elective -I 1. Advancement in Networking 2. Machine Learning 3. Foundation of Cyber Security 4. Courses in association with industries	3	-	1	1	3	30	20	50	-	-
7.	RM	<tbd>	Research Methodology and Intellectual Property Rights	3	-	-	1	3	30	20	50	-	-
Total Credits				25									

Legends:

L-Lecture, T-Tutorial, P-Practical, S-Self Study, Cr-Credits,

ISE: In-Semester-Evaluation, ESE: End-Semester-Evaluation, MSE: Mid-Semester Evaluation, TA: Teacher's Assessment, CIE: Continuous-Internal-Evaluation

Semester II

Sr. No.	Course Type	Course Code	Course Name	L	T	P	S	Cr	Evaluation Scheme (Weightages in %)				
									Theory			Laboratory	
									MSE	TA	ESE	ISE	ESE
1.	OE	<tbd>	Open Elective	3	-	-	1	3	30	20	50	-	-
2.	PCC	<tbd>	Network Security	3	-	2	1	4	30	20	50	50	50
3.	PCC	<tbd>	Digital Forensics and Data Recovery	3	-	2	1	4	30	20	50	50	50
4.	PCC	<tbd>	Wireless Networks & Security	3	-	2	1	4	30	20	50	50	50
5.	PEC-2	<tbd>	Programme Elective -II 1. Blockchain Technology 2. Quantum Cryptography 3. Cloud Computing and Security 4. Courses in association with industries	3	-	-	1	3	30	20	50	-	-
6.	PEC-3	<tbd>	Programme Elective -III 1. Web Security 2. Internet of Things and Security 3. Vulnerability Assessment & Penetration Testing 4. Courses in association with industries	3	-	-	1	3	30	20	50	-	-
7.	AEC	<tbd>	Effective Technical Communication Skills and Self Awareness	1	-	2	1	2	50	50	-	100	
8.	LLC	<tbd>	Liberal Learning Course	-	-	2	2	1	-	-	-	100	-
Total Credits				24									

- The department offers “Data Structures” as Open Elective for students of other departments.
- Exit option to qualify for PG Diploma in Computer Science and Inforesearch
- Information Security:
    - Eight weeks domain-specific industrial internship in the month of June-July after successfully completing the first year of the program

Semester III

Sr. No.	Course Type	Course Code	Course Name	L	T	P	S	Cr	Evaluation Scheme (Weightages in %)				
									Theory			Laboratory	
									MSE	TA	ESE	ISE	ESE
1	SLC	<tbd>	Massive Open Online Course –I	3	-	-	1	3	-	-	100	-	-
2	SLC	<tbd>	Massive Open Online Course –II	3	-	-	1	3	-	-	100	-	-
3	OJT	<tbd>	Internship	-	-	-	-	3	-	-	100	-	-
4	Project	<tbd>	Dissertation Phase – I	-	-	22	12	11	-	-	-	70	30
Total Credits				20									

Semester IV

Sr. No.	Course Type	Course Code	Course Name	L	T	P	S	Cr	Evaluation Scheme (Weightages in %)				
									Theory			Laboratory	
									MSE	TA	ESE	ISE	ESE
1	Project	<tbd>	Dissertation Phase – II	-	-	22	12	11	-	-	-	70	30
Total Credits				11									

[PSQT] 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) : 20 Marks
End Sem. Exam (ESE) : 50 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.

Basic Probability Theory **[2 Hrs]**

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

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

Stochastic Processes **[6 Hrs]**

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

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

Statistical Inference **[8 Hrs]**

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

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
Lectures : 2 hrs/week
Lab: 2 hrs/week
Self-Study : 1 hr/week

Examination Scheme
Mid Sem. Exam (MSE) : 30 marks
Teachers Assessment (TA) : 20 Marks
End Sem. Exam (ESE) : 50 Marks
Lab: CIE: 50 marks, ESE: 50 Marks

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 problem, reduce problems and argue about complexity classes

Mathematical Foundation **[6 Hrs]**

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

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.

Standard Design Techniques-I **[6 Hrs]**

Divide and Conquer, Greedy method.

Standard Design Techniques-II **[8 Hrs]**

Dynamic programming, Graphs and Traversals.

Standard Design Techniques-III **[6 Hrs]**

Backtracking, Branch-and-bound.

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

Self-Study:

Sorting in linear time, Elementary graph algorithms, Minimum spanning tree, Number -Theoretic algorithms: GCD algorithm, Chinese remainder theorem, Primality testing, String Matching Algorithms

Text Books

• Ellis Horowitz, Sartaj Sahni and Sanguthevar Rajasekaran, "Fundamentals of Computer Algorithms", Universities Press, 2nd edition (2008) , ISBN-13: 978- 8173716126
• Thomas Cormen, Charles Leiserson, Ronald Rivest and Cliford Stein, "Introduction to Algorithms", PHI, 3rd edition, ISBN-13: 978-8120340077

Reference Books

• Gilles Brassard and Paul Bratley, "Fundamentals of Algorithmics", PHI, ISBN-13: 978-

8120311312
• Jon Kleinberg and Éva Tardos, “Algorithm Design”, Pearson Education India, ISBN13: 978-9332518643

Suggested List of Assignments in the Laboratory:
Lab sessions will consist of solving numerical problems based on the algorithms discussed in theory lectures, discussions around finding complexities and analysis of algorithms.

1. Recurrence Relations
• Study and solve recurrence relations using formal methods such as substitution, recursion tree, and the Master Theorem to determine algorithmic time complexities.

2. Sorting Algorithm Analysis
• Implement, trace, and analyze the performance of advanced sorting algorithms including Heap Sort, Quick Sort, and Merge Sort, with emphasis on time complexity in best, worst, and average cases.

3. Greedy Strategy Implementation
• Design and implement greedy algorithms to solve problems such as Fractional Knapsack, Job Sequencing with Deadlines, Huffman Coding, and Optimal Merge Pattern. Analyze correctness and efficiency.

4. Graph Algorithms
• Develop and evaluate graph-based solutions including: Single-source shortest path using Dijkstra’s algorithm, Minimum Spanning Tree construction using Prim’s and Kruskal’s algorithms.

5. Dynamic Programming Techniques
• Implement dynamic programming solutions for classical problems:Matrix Chain Multiplication, Longest Common Subsequence (LCS), 0/1 Knapsack, All-Pairs Shortest Paths using Floyd-Warshall algorithm, Bellman-Ford algorithm for single-source shortest paths.

6. String Matching Algorithms
• Implement and analyze the performance of pattern matching algorithms including the Naive approach and Knuth-Morris-Pratt (KMP) algorithm.

7. Branch and Bound Applications
• Apply the branch-and-bound strategy to solve computationally hard problems such as the 0/1 Knapsack and Travelling Salesperson Problem (TSP), focusing on pruning and bounding techniques.

8. Backtracking Approaches
• Solve combinatorial problems using backtracking techniques, including: N-Queens Problem, Graph Coloring, Hamiltonian Path,Travelling Salesperson Problem (exact approach)

9. Network Flow Algorithms
• Implement and analyze network flow algorithms such as: Ford-Fulkerson method, Push-Relabel algorithm and evaluate their time complexity and applicability.

10. NP-Completeness and Reductions
• Apply polynomial-time reduction techniques to prove the NP-completeness of selected decision problems, understanding the significance of complexity classes and intractability.

[PCC] Principles of Cryptography

Teaching Scheme
Lectures : 3 hrs/week
Self-Study : 1 hr/week

Examination Scheme
Mid Sem. Exam (MSE) : 30 Marks
Teachers Assessment (TA) : 20 Marks
End Sem. Exam (ESE) : 50 Marks

Course Outcomes:

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

1. Understand various security services, security attacks and classical encryption techniques
2. Apply the concepts of finite mathematics and number theory.
3. Able to acquire knowledge about the background mathematics of symmetric key cryptography and understand, analyse and implement the symmetric key algorithm.
4. Understand and Implement the asymmetric encryption algorithms,the concept of message integrity and the algorithms for checking the integrity of data.

Introduction **[6 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. One Time Pad.

Classical Encryption Techniques **[7 Hrs]**

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

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.

Symmetric 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), International Data Encryption Algorithm (IDEA), Differential and Linear cryptanalysis, Weak Keys.

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.

Hashing and Digital Signature **[6 Hrs]**

Cryptographic Hash functions: Message Digest 5 (MD5), Secure Hash algorithm (SHA), Message Authentication Codes, Digital Signature Algorithm.

Self Study:

RC5, International Data Encryption Algorithm (IDEA), Differential and Linear cryptanalysis

Text Books

1. "Cryptography and Information Security", V. K. Pachghare, 3rd edition, PHI Learning,

ISBN: 978-93-89-347-10-4.
2. “Cryptography and Network Security, Principles and Practice”, William Stallings, Pearson Education, Seventh Edition, and ISBN: 978-93-325-8522-5

Reference Books

1. “Network Security the Complete Reference”, Robert Bragge, Mark Rhodes, Heith Straggberg· Tata McGraw Hill Publication, ISBN: 9780072226973.
2. “Network Security: Private Communication in a Public World”, Charlie Kaufman, Radia Perlman, and Mike Speciner, Prentice Hall, ISBN 0-13-046019-2.

[PCC & LC] Computer Systems 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) : 20 Marks
End Sem. Exam (ESE) : 50 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.

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.

Database Security [05 Hrs]
The Need for Database Security, Database Management Systems, Relational Databases, SQL Injection Attacks, Database Access Control, Inference, Database Encryption.

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.

Software Security [07 Hrs]
Software Security Issues, Handling Program Input, Writing Safe Program, Code, Interacting withthe Operating System and Other Programs, Handling Program Output.

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

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] Information Theory and Coding

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) : 20 Marks
End Sem. Exam (ESE) : 50 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.

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.

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.

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.

Network Coding [07 Hrs]
The Buttery Network, Wireless and Satellite Communications, Source Separation, the Max-FlowBound, Single-Source Linear Network Coding: Acyclic Networks.

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

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
Lectures : 3 hrs/week
Self-Study : 1 hr/week

Examination Scheme
Mid Sem. Exam (MSE) : 30 marks
Teachers Assessment (TA) : 20 Marks
End Sem. Exam (ESE) : 50 Marks

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

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

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

Socket Programming Fundamentals [07 Hrs]
Sockets Introduction, Elementary TCP Sockets, IO Multiplexing, Socket Options, Elementary UDP Sockets, elementary SCTP Sockets.

Advanced Socket Programming and I/O Models [07 Hrs]
Advanced Sockets, Daemon Processes and the Inetd Superserver, Advanced IO Options,Non blocking I/O.

Advanced Network Programming and IP Mechanisms [08 Hrs]
Routing Sockets, Broadcasting, Multicasting, Advanced UDP Sockets, Raw Sockets,Out-of-Band Data, Signal Driven IO, IP Options, Data Link Access.

Modern Networking [06 Hrs]
Storage and Networking, Software Defined Networks, Open Stack Networking, Neutron.

Self Study: Network Security and Emerging Networking Technologies
SSL/TLS and Secure Socket Programming, Firewalls and Intrusion Detection Systems, Virtual Private Networks (VPN), Network Function Virtualization (NFV), Introduction to Cloud Networking and Container Networking

TEXT BOOKS:

1. Computer Networks: A Systems Approach, 4e. Larry L. Peterson and Bruce
2. S. Davie, Publisher: Morgan Kaufmann; 4 edition (March 22, 2007), ISBN-10: 0123705487, ISBN-13: 978-0123705488
3. 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
4. Tom Clark, Designing Storage Area Networks, A Practical Reference for ImplementingFibre Channel and IP SANs, Addison-Wesley Professional, 2nd Edition, 2003.
5. Open Stack Cloud Computing Cookbook, 2nd Edition, Kevin Jackson , Cody Bunch, PacktPublishing, 978-1-78216-758-7

[PEC] Machine Learning

Teaching Scheme
Lectures : 3 hrs/week
Self-Study : 1 hr/week

Examination Scheme
Mid Sem. Exam (MSE) : 30 marks
Teachers Assessment (TA) : 20 Marks
End Sem. Exam (ESE) : 50 Marks

Course Outcomes:

Students will be able to:-

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

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.

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

Data Forms- Data, information, kinds of data Input - Concepts: instances and attributes Output - Knowledge Representation: vector space model, decision tree or instance-based representation. Preprocessing - For Numeric kind of data, For text kind of data

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

Classification, Probabilistic classifier **[08 Hrs]**

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

Decision Trees and Clustering **[08 Hrs]**

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

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] Foundation of Cyber Security

Teaching Scheme
Lectures : 3 hrs/week
Self-Study : 1 hr/week

Examination Scheme
Mid Sem. Exam (MSE) : 30 marks
Teachers Assessment (TA) : 20 Marks
End Sem. Exam (ESE) : 50 Marks

Course Outcomes:

Students will be able to:

1. Define the need of Cyber Security.
2. Explain the IT act, Application Security vulnerabilities and its mitigation techniques.
3. Demonstrate the knowledge of penetration testing, and social networking security.
4. Analyse the malwares, social networking websites and impact of cyber-crime on ecommerce.

Introduction: **[6 Hrs]**

Nature and scope of computer crime, Understanding how cyber criminals and hackers work, Different types of cyber-crimes, Introduction to digital signatures, Cryptography, Digital certificate and public key infrastructure, IT Act., Impact of cyber-crime on e-governance and e-commerce.

Malware reverse engineering: **[6 Hrs]**

Overview of malware reverse engineering, Types of malware, Malicious code families, Latest trends in malware analysis, Basic static and dynamic analysis, Malware analysis techniques, Case study.

Web application security: **[8 Hrs]**

Introduction to web application security: Attacks, vulnerabilities and mitigation, Client-side security, Server-side security, Application security: HTTPS, HSTS etc., Security engineering: Passwords and their limitations, Attacks on passwords: CAPTCHA, OTP. Advanced security topics: Secure email systems: PGP, SMIME, DKIM, DMARC, DNSSec, SMTP STS etc., Privacy and security for online social networks, Database security, Browser security, Mobile device security.

Ethical hacking and penetration testing: **[8 Hrs]**

Security Technologies: IDS, IPS, Ethical hacking, Penetration testing fundamentals: Reconnaissance, scanning, gaining access, maintaining access, Covering tracks. Concept of Cyberspace & Netizens, Objective & Scope of the Information Technology Act, Comparisons between traditional criminal techniques and Cyber Crime, Public and Private Societies face challenges in addressing cybercrime, Computer Hardware, Networks and Internet: An Introduction.

Nature and scope of computer crime, Understanding how cyber criminals and hackers work, types of cyber crime: **[6 Hrs]**

Financial crime, cyber pornography, Forgery, Web Defacement, Data Diddling, Email frauds, Hacking, Tempering, Spamming, Phishing, Spoofing, Pharming, DoS Attacks, Viruses, Trojan, Worm, Malware, Spyware, Botnet etc. Concept of Digital Signatures and

Cryptography, Digital Signature Certificate and Public Key Infrastructure. Authorities under the IT Act., Impact of cyber crime on e-governance and e-commerce.

Cyber crime & Computer-based electronic and Digital evidence: [6 Hrs]

Indian law perspective, Procedure for search & Seizure, Best practices for cyber crime Investigations involving the Computer, Internet and Networks: E-mail, Websites, Chatrooms, file sharing, Network Intrusion/Denial of Services, Messages boards, password breaking, keyloggers, IP tracing, etc. Case studies: Cloud security, Operating system security, Security of social networking websites, IoT devices security, E-commerce websites security.

Text Books:

1. Hossein, "Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management", Wiley, Volume 3 edition, ISBN-13: 978-0470323069.
2. Georgia Weidman, "Penetration testing: A Hands-On Introduction to Hacking", No Starch Press, 2014, ISBN-13: 978-1593275648.
3. Michael Sikorski and Andrew Honig, " Practical Malware Analysis", No Starch Press, 1st Edition, 2012, ISBN-13: 978-1593272906

Reference Books:

1. "Practical Internet of Things Security" by Brian Russell, Drew Van Duren, Packt publishing, 2016, ISBN: 9781785889639
2. T. Mather, S. Kumaraswamy, S. Latif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance", O'Reilly Series, 2009, ISBN-13: 978- 0596802769.
3. "Cyberlaw: the Indian perspective"; Pavan Duggal; Saakshar Law Publications, 1st edition, 2002, ISBN: 8189121022, 9788189121020.

[RM] Research Methodology and Intellectual Property Rights

Teaching Scheme	Examination Scheme
Lectures: 3 hours/week	Theory: CIE: 30 Marks, TA: 20 marks
Self-Study: 1 hour/week	ESE: 50 Marks

Course Outcomes (COs):

Students will be able to

1. Formulate research problems by defining objectives, hypotheses, variables, and feasibility.
2. Synthesize literature using reproducible search and screening strategies.
3. Apply research ethics, authorship norms, compliance rules, and FAIR data practices.
4. Produce research outputs through ethical analysis, documentation, and dissemination.

Introduction to Research **[4 hrs]**

What is scientific research, objectives of research, motivation, types of research, research approaches, research methodology, significance of research, indications of good research

Designing a Problem **[6 hrs]**

Research problems, formulation of feasible problem, hypothesis, errors in problem selection, selection of variables

Methods- Simulations and Experiments **[7 hrs]**

Conventional approaches, selection of tools, setting up production, validation of results, performance analysis, sensitivity analysis, and errors in measurements

Statistics and Uncertainty Quantification **[7 hrs]**

Data, importance of analyzing data, types of analyses, selection practices, statistics, sampling techniques, uncertainty quantification, errors analysis

RCR and Ethics **[5 hrs]**

Responsible conduct of research, IEC compliance, what is plagiarism, QRPs, generative A.I. in research

IPR, Research Ethics and Publishing **[5 hrs]**

Introduction to IPR, significance of IPR, types of IPR, recent developments, technical writing

Reference Books:

1. Melville, S., & Goddard, W. (1996). Research methodology: An introduction for science & engineering students. Juta & Co.
2. Kothari, C. R. (2009). Research methodology: Methods and trends. New Age International Publishers.
3. Goddard, W., & Melville, S. (2001). Research methodology: An introduction (2nd ed.). Juta Academic.
4. Kumar, R. (2005). Research methodology: A step-by-step guide for beginners (2nd ed.). Sage Publications.
5. Sharma, S. D. (2001). Operational research. Kedar Nath Ram Nath & Co.

Semester II

[OE] Data Structures

Teaching Scheme
Lectures : 3 hrs/week
Self-Study : 1 hr/week

Examination Scheme
Mid Sem. Exam (MSE) : 30 marks
Teachers Assessment (TA) : 20 Marks
End Sem. Exam (ESE) : 50 Marks

Course Outcomes

Students will be able to:

1. Understand and use the basic concepts for algorithm complexity
2. Use advanced data structures for efficient searching
3. Employ various data structures for implementing priority queues.
4. Analyze the time and space complexity string data structures.
5. Use different data structures to solve graph problems.
6. Design solutions for real-life problems using appropriate data structures.

Algorithm Concepts **[8 Hrs]**

Abstract data types, Data structures, Algorithms, Big Oh, Small Oh, Omega and Theta notations, solving recurrence equations, Master theorems, Generating function techniques, Constructive induction.

Advanced Search Structures for Dictionary ADT **[8 Hrs]**

Splay trees, Amortized analysis, 2-3 trees, 2-3-4 trees, Red-black trees, Randomized structures, Skip lists, Treaps, Universal hash functions.

Advanced Structures for Priority Queues **[6 Hrs]**

Binary Heap, Min Heap, Max Heap, Binomial heaps, Leftist heaps, Skewed heaps, Fibonacci heaps and its amortized analysis, Applications to minimum spanning tree algorithms.

Data Structures for Strings **[8 Hrs]**

Introduction to string data structures, Huffman coding tree, Tries, Compressed Tries, Suffix Trees, Suffix Arrays; Applications-Search Engines, Bioinformatics, Pattern Matching: KMP algorithm; Internet Packet Forwarding.

Graph Algorithms **[6 Hrs]**

BFS, DFS, Disjoint set union problem, Network flow; Maximum-Flow / Minimum-Cut; Ford–Fulkerson algorithm, Hamiltonian Path and circuit problem, Introduction to Hypergraphs.

Self-study

Geometric data structures, Cut vertices, Plane sweep paradigm, Hamiltonian Path and circuit problem.

Text Books:

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

References:

1. S. Dasgupta, C.H. Papadimitriou, and U. V. Vazirani, Algorithms, McGraw-Hill, 2006; ISBN- 13: 978-0073523408 ISBN-10: 007352340, 2
2. J. Kleinberg and E. Tardos, Algorithm Design, 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) : 20 Marks
End Sem. Exam (ESE) : 50 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

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

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

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).

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.

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

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.

Self Study
Federated Identity Management, SHA-512, Message Authentication Code (MAC), HMAC, Comparison of Kerberos with SSL, ISAKMP Protocol, OAKLEY Protocol, Dark web, Wireless Network Security.

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) : 20 Marks
End Sem. Exam (ESE) : 50 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

Introduction: **[8 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.

Digital Evidence Acquisition: **[8 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.

MS Windows Forensics: **[8 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

Windows File Systems: **[8 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.

Email Forensics: **[8 Hrs]**
Email Structure, working, Email Protocols, Examining email messages, Email Server Examination, Tracing emails, Email Forensics Tools

Self Study:
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.

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 Network and 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) : 20 Marks
End Sem. Exam (ESE) : 50 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

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.

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.

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.

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.

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.

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
Lectures : 3 hrs/week
Self-Study : 1 hr/week

Examination Scheme
Mid Sem. Exam (MSE) : 30 marks
Teachers Assessment (TA) : 20 Marks
End Sem. Exam (ESE) : 50 Marks

Course Outcomes:

Student will be able to

1. Explain fundamental concepts, history, and applications of blockchain technology.
2. Apply cryptographic principles to ensure security and integrity in blockchain systems.
3. Analyze blockchain components, consensus mechanisms, and major cryptocurrencies.
4. Design and implement basic smart contracts and DApps using Ethereum.
5. Compare and evaluate enterprise blockchain platforms with emphasis on Hyperledger Fabric.
6. Assess emerging blockchain technologies and real-world use cases across industries.

Introduction to Blockchain Technology **[8 Hrs]**

Basic ideas behind block chain, Why blockchain, History of Blockchain, how it is changing the landscape of digitalization, Applications of Blockchain, Benefits of Blockchain in business, Transaction cycle in Blockchain.

Cryptographic Foundations **[8 Hrs]**

Cryptographic hash functions (SHA-256, Merkle Trees), Digital signatures, Public key and private key cryptography, Hash pointers and data integrity, Wallets and address generation, Security concepts in Blockchain.

Components of Blockchain and Cryptocurrencies **[8 Hrs]**

Types of Block chains: Permission & Permission less Block chains, Blockchain Consensus, Types of networks, Mining, Tokenization in Blockchain, Cryptocurriencies: Bitcoin, Ethereum, Litecoin and Dodge Coin.

Blockchain Platform Ethereum **[8 Hrs]**

Ethereum architecture, Smart contracts, Solidity basics, Gas, Ethereum Virtual Machine, and contract execution, Decentralized Applications (DApps), Decentralized Autonomous Organization (DAO).

Blockchain Platform Hyper ledger **[8 Hrs]**

The Architecture of Hyper ledger Fabric System, features of a Hyper ledger blockchain, working of Hyper ledger Fabric, Benefits of Hyper ledger Fabric, Differences Between Ethereum And Hyper ledger.

Emerging Trends in Blockchain **[8 Hrs]**

Cloud-based block chain, Multi chain, Geth , Stellar , Ripple, R3 Corda, Blockchain API, NFTs,DeFi.

Self Study: Block Chain Use Cases

Supply Chain Management, Finance, Health Care, Internet of Things (IoT), Remittance, Land Records,Voting and election, Loyalty Programs, Go Green (Renewable Energy).

Text Books:

1. Artemis Caro, “Blockchain: The Beginners Guide to Understanding the Technology behind Bitcoin
& Crypto currency”.
2. Scott Marks, “Blockchain for Beginners: Guide to Understanding the Foundation and Basics of the
Revolutionary Blockchain Technology”, Create Space Independent Publishing Platform

Reference Books:

1. Mark Watney, “Blockchain for Beginners”.
2. Alwyn Bishop, “Blockchain Technology Explained”

Web references

1. NPTEL Course “Introduction to Blockchain Technology & Applications”
https://nptel.ac.in/courses/106/104/106104220/
2. NPTEL Course on “Blockchain Architecture &Use Cases”
https://nptel.ac.in/courses/106/105/106105184/

[PEC] Quantum Cryptography

Teaching Scheme:
Lectures : 3 Hrs/week
Tutorial: 1 Hr/week

Examination Scheme:
TA – 20 marks
MSE – 30 marks
ESE - 50 marks

Course Outcomes:

Students will be able to:

1. Explain the foundational principles of quantum mechanics and quantum information relevant to quantum cryptography.
2. Demonstrate and compare various Quantum Key Distribution (QKD) protocols and their operational principles.
3. Analyze security vulnerabilities and attack strategies in quantum cryptographic systems.
4. Evaluate the practical limitations and performance trade-offs in real-world quantum cryptography implementations.
5. Critique the scope, challenges, and future directions of quantum cryptography in comparison to classical and post-quantum cryptographic systems.

Foundations of Quantum Mechanics: Limitations of classical cryptography, Post-quantum threats & motivation for quantum cryptography, Qubits and quantum states, Superposition and probability amplitudes, Measurement postulate, Heisenberg uncertainty principle **[5 Hrs]**

Quantum Information Basics: Dirac notation ($|0\rangle$, $|1\rangle$, superposition states), Density matrices (pure vs mixed states), Quantum entanglement, Bell states, Bell's inequality and non-locality**.** **[6 Hrs]**

Quantum Key Distribution (QKD) : Principles of Quantum Key Distribution, BB84 protocol, B92 protocol, E91 (Entanglement-based) protocol, Sifting, error correction, and privacy, amplification, Intercept-resend attack, Photon-number-splitting (PNS) attack **[6 Hrs]**

Practical Quantum Cryptography: Decoy-state QKD, Quantum channels (optical fiber & free-space), Sources and detectors (single-photon sources, SPDs), Quantum repeaters (basic idea), Signal loss, noise, and decoherence **[8 Hrs]**

Security and Attacks: Security proofs of QKD (basic concepts), Eavesdropping strategies, Side- channel attacks, Trojan-horse attacks, Device-independent QKD **[8 Hrs]**

Applications and Future Directions: Quantum cryptography vs classical cryptography, Commercial QKD systems, Satellite-based QKD, Quantum networks, Integration with classical networks, Challenges and future research directions **[8 Hrs]**

Self Study:

No-cloning theorem, Bell's inequality and non-locality, Quantum randomness, Signal degradation and distortion, Measurement-device-independent QKD and Challenges and future research directions

Text Books:

1. **Quantum Communications and Cryptography** (edited by Alexander V. Sergienko) — a comprehensive review of theory and practical implementations, including entanglement, QKD, and experimental systems.
2. **Quantum Communication and Cryptography** by Walter O. Krawec — (upcoming/2026) text focused on the theory of quantum cryptography, QKD protocols, security proofs, and practical considerations.

Reference Books:

3. **Design and Analysis of Secure Quantum Communication Schemes** — modern Springer book covering security and analysis of quantum secure communication systems (protocols, quantum key agreement, private queries).
4. **Quantum Private Communication** by Guihua Zeng — covers fundamentals of quantum private communication and secure quantum systems alongside implementation details.

[PEC] Cloud Computing and Security

Teaching Scheme
Lectures : 3 hrs/week
Self-Study : 1 hr/week

Examination Scheme
Mid Sem. Exam (MSE) : 30 marks
Teachers Assessment (TA) : 20 Marks
End Sem. Exam (ESE) : 50 Marks

Course Outcomes:
Student will be able to

1. Understand fundamentals of cloud computing architectures based on current standards, protocols, and best practices intended for delivering Cloud based enterprise IT services and business applications.
2. Identify the known threats, risks, vulnerabilities and privacy issues associated with 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.

Fundamentals of Cloud Computing and Architectural Characteristic [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.

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.

Secure Isolation of Physical & Logical Infrastructure [6 Hrs] Isolation - Compute, Network and Storage, Common attack vectors and threats, Secure Isolation Strategies – Multi-tenancy, Inter-tenant network segmentation strategies, Storage isolation strategies.

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, Assuring data deletion, Data retention, deletion and archiving procedures for tenant data, Data Protection Strategies.

Enforcing Access Control for Cloud Infrastructure based Services [7 Hrs]
Understand the access control requirements for Cloud infrastructure, Common attack vectors and threats, - Authentication and Authorization, Roles-based Access Control, Multifactor authentication, Host, storage and network access control options, OS Hardening and minimization, securing remote access,

Monitoring, Auditing and Management [7 Hrs]
Auditing – Record generation, Reporting and Management, Tamper-proofing audit logs, Quality of Services, Secure Management - User management, Identity management,

Self-study Topics:
Virtualization strategies, Encryption, Data Redaction, Tokenization, Obfuscation, PKI and Key Management, Verified and measured boot, Firewalls, IDS, IPS and honeypots, Security Information and Event Management., Enforcing Access Control Strategies - Compute, Network and Storage, Proactive activity monitoring, Incident Response, Monitoring for unauthorized access, malicious traffic, abuse of system privileges, intrusion detection, events and alerts.

Text Books:

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

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

Reference Books:

1. 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) : 20 Marks
End Sem. Exam (ESE) : 50 Marks

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

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

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

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

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

Self Study
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 and Security

Teaching Scheme
Lectures : 3 hrs/week
Self-Study : 1 hr/week

Examination Scheme
Mid Sem. Exam (MSE) : 30 marks
Teachers Assessment (TA) : 20 Marks
End Sem. Exam (ESE) : 50 Marks

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.

Introduction to IoT and Web of Things Architecture [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.

IoT Architecture and Reference Models [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.

IoT Security: Classification and Access Control [6 Hrs]

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

IoT Security, Privacy, and Policy Frameworks [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

IoT Attacks and Secure Implementation [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.

IoT Security Protocols and Management [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

Self Study: Applications and Case Studies

Home automations – Smart cities – Environment – Energy – Retail – Logistics – Agriculture – Industry – Health and lifestyle – Case study.

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

[PEC] Vulnerability Assessment and Penetration Testing

Teaching Scheme
Lectures : 3 hrs/week
Self-Study : 1 hr/week

Examination Scheme
Mid Sem. Exam (MSE) : 30 marks
Teachers Assessment (TA) : 20 Marks
End Sem. Exam (ESE) : 50 Marks

Course outcomes:
At the end of the course, the student will be able to:

1. Explain the ethical considerations and legal implications in conducting ethical hacking activities using appropriate tools.
2. Analyze social engineering, physical penetration and insider attacks using automating penetration testing processes.
3. Identify report penetration tests effectively to develop and execute Linux and Windows exploits, by passing memory protections.
4. Illustrate web application security vulnerabilities to conduct vulnerability analysis.
5. Inspect protection against client-side browser exploits.

Introduction to Ethics of Ethical Hacking: Why You Need to Understand Your Enemy's Tactics, Recognizing the Gray Areas in Security, Vulnerability Assessment and Penetration Testing.
Penetration Testing and Tools: Social Engineering Attacks: How a Social Engineering Attack Works, Conducting a Social Engineering Attack, Common Attacks Used in Penetration Testing, Preparing Yourself for Face-to-Face Attacks, Defending Against Social Engineering Attacks. **[8 Hrs]**

Physical Penetration Attacks: Need of Physical Penetration, Conducting a Physical Penetration, Common Ways into a Building, Defending Against Physical Penetrations.
Insider Attacks: Conducting an Insider Attack, Defending Against Insider Attacks.
Metasploit: The Big Picture, Getting Metasploit, Using the Metasploit Consoleto Launch Exploits, Exploiting Client-Side Vulnerabilities with Metasploit, Penetration Testing with Metasploit's Meterpreter, Automating and Scripting Metasploit, Going Further with Metasploit. **[8 Hrs]**

Managing a Penetration Test: Planning a Penetration Test, Structuring a Penetration Testing Agreement, Execution of a Penetration Test, Information Sharing During a Penetration Test, Reporting the Results of a Penetration Test
Basic Linux Exploits: Stack Operations, Buffer Overflows, Local Buffer Overflow Exploits, Exploit Development Process
Windows Exploits: Compiling and Debugging Windows Programs, Writing Windows Exploits, Understanding Structured Exception Handling (SEH), Understanding Windows Memory Protections (XP SP3, Vista 7 And Server 2008), Bypassing Windows Memory Protections. **[8 Hrs]**

Web Application Security Vulnerabilities: Overview of Top Web Application Security Vulnerabilities, Injection Vulnerabilities, Cross-Site Scripting Vulnerabilities, The Rest of the OWASP Top Ten, SQL Injection Vulnerabilities, Cross-Site Scripting Vulnerabilities. Vulnerability Analysis: Passive Analysis: Source Code Analysis, Binary Analysis. **[8 Hrs]**

Client-Side Browser Exploits: Why Client-Side Vulnerabilities are Interesting, Internet Explorer Security Concepts, History of Client-Side Exploits and Latest Trends, Finding New Browser-Based Vulnerabilities, Heap Spray to Exploit, Protecting Yourself from Client-Side Exploit.
Malware Analysis: Collecting Malware and Initial Analysis: Malware, Latest Trends in Honeynet Technology, Catching Malware: Setting the Trap, Initial Analysis of Malware. **[8 Hrs]**

Suggested Learning Resources:

Textbook:

1. Gray Hat Hacking, The Ethical Hackers Handbook, Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, and Terron Williams, 3rd Edition, Tata McGraw-Hill.
2. Rafay Baloch, Ethical Hacking and Penetration Testing Guide, CRC Press Taylor & Francis Group

Reference Books:

1. The Web Application Hacker's Hand Book - Discovering and Exploiting Security flaws, Dafydd Suttard, Marcuspinto,1st Edition, Wiley Publishing.
2. Penetration Testing: Hands-on Introduction to Hacking, Georgia Weidman, 1st Edition, No 5, Starch Press.
3. The Pen Tester Blueprint - Starting a Career as an Ethical Hacker, L. Wylie, Kim Crawly,1st Edition, Wiley Publications.

Additional Learning Recourses:

Web links and Video Lectures(e-Resources):

1. https://www.youtube.com/watch?v=fgdcE4kfQBc
2. https://www.youtube.com/watch?v=bQh-nhhYcS4
3. https://www.youtube.com/watch?v=i5GLg9XWJg4
4. https://ieeexplore.ieee.org/document/8463920
5. https://qualysec.com/penetration-testing-and-vulnerability-assessment/

[CCA] Liberal Learning Course

Teaching Scheme
Lectures: 1 hour/week

Examination Scheme
CIE: 90 marks, TA: 20 marks

Guidelines:

Liberal Learning Courses began aims with a vision of expanding the horizons of knowledge in a variety of areas beyond Engineering. It provides opportunities to students of Engineering to foray into areas of their interest, to contribute to their overall personality development. The students are required to go through the areas of agriculture, Clay Art & Pottery, Dance (Contemporary), Dance (Indian), Film Appreciation, French, Geography, Holistic Health, Interior Design, Introduction to Indian Armed Forces, Music (Instrumental), Music (Vocal), Painting, Photography, Political Science, Theatre & Dramatics, Wood & Metal Art etc.

Experts from respective areas conduct classes for each area on campus through activities, discussions, presentations, and lecture methods, and an evaluation out of 100 per area is done for each area throughout the semester. Evaluation patterns may differ according to the nature of each area. Although there is no pre-defined syllabus for LLC areas, there is an outline that experts normally develop and follow for the classes. However, students may approach the faculty to cover certain topics of their interest in that area during classes based on students' interests and experts' areas of expertise.

[MLC] Effective technical communication skills and Self awareness

Teaching Scheme
Lectures: 1 hour/week
Self-Study: 1 hour/week

Examination Scheme
Theory: CIE: 90 Marks
TA: 20 marks

Course Outcomes (COs):

Students will be able to

1. Produce effective dialogue for business related situations
2. Use listening, speaking, reading and writing skills for communication purposes and attempt tasks by using functional grammar and vocabulary effectively
3. Analyze critically different concepts/principles of communication skills
4. To appreciate, analyze, and evaluate business reports and research papers

Fundamentals of Communication **[4 hrs]**

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

Aural-Oral Communication **[4 hrs]**

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

Reading and Writing **[4 hrs]**

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

Text Books

1. Raman Sharma, "Technical Communication", Oxford University Press.
2. Raymond Murphy "Essential English Grammar" (Elementary & Intermediate) Cambridge University Press.
3. Mark Hancock "English Pronunciation in Use" Cambridge University Press.
4. Shirley Taylor, "Model Business Letters, Emails and Other Business Documents" (seventh edition), Prentice 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, Cambridge University Press
2. C. E. Shannon, A Mathematical Theory of Communication, Bell Sys. Tech Journ, 1948.

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

Detailed Syllabus: Semester III

[SLC] Massive Open Online Course – I

Teaching Scheme	Examination Scheme
Self-Study: 3hours / Week	CIE: 50 Marks, ESE: 50 marks

Course Outcome

Students will be able to:

1. Acquire new skills or knowledge to enhance their personal and professional development
2. Receive a flexible learning environment, allowing one to study at own pace and convenience
3. Opportunity for lifelong learning
4. Foster collaboration and networking among participants

The students in consultation with the faculty advisor, opt for a single course of 12 weeks offered by the NPTEL in the current semester. The students need to register for the examination conducted by the NPTEL. For the students who secured a passing score in the NPTEL examination, the marks obtained for assignments (in 25 marks) will be upscaled to out of 50 marks of CIE and the marks obtained from the certificate examination (in 75 marks) will be downscaled 50 marks of ESE assessments.

[SLC] Massive Open Online Course – II

Teaching Scheme	Examination Scheme
Self-Study: 3 hours / Week	CIE: 50 Marks, ESE: 50 marks

Course Outcome

Students will be able to:

1. Acquire new skills or knowledge to enhance their personal and professional development
2. Receive a flexible learning environment, allowing one to study at own pace and convenience
3. Opportunity for lifelong learning
4. Foster collaboration and networking among participants

The students in consultation with the faculty advisor opt for a single course of 12 weeks offered by the NPTEL in the current semester. The students need to register for the examination conducted by the NPTEL. For the students who secured a passing score in the NPTEL examination, the marks obtained for assignments (in 25 marks) will be upscaled to out of 50 marks of CIE and the marks obtained from the certificate examination (in 75 marks) will be downscaled 50 marks of ESE assessments.

[Project] Dissertation Phase – I

Teaching Scheme	Examination Scheme
Laboratory: 22 hours/week	Theory: CIE: 70 Marks
Self-Study: 12 hours / Week	**ESE: 30 marks**

Course Outcomes

Students will be able to:

1. Demonstrate how to search the existing literature to gather information about a specific problem or domain.
2. Identify the state-of-the-art technologies and research in the chosen domain and highlight open problems that are relevant to societal or industrial needs.
3. Evaluate various solution techniques to determine the most feasible solution within the given constraints for the chosen dissertation problem.
4. Apply software engineering principles related to requirements gathering and design to produce relevant documentation.
5. Write a dissertation report that details the research problem, objectives, literature review, and solution architecture.
6. Deliver effective oral presentations to communicate the findings and outcomes of the research work.

Guidelines

The dissertation is a year-long project, conducted and evaluated in two phases. It can be carried out either in-house or within an industry as assigned by the department. The project topic and internal advisor (a faculty member from the department) are determined at the beginning of Phase I.

Students are 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 the 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 (preferably, but not mandatory)

Evaluation

Two independent assessments (Mid-Semester and End-Semester evaluations) will be made. In both the Examinations, the internal guide, along with a Senior Faculty member of the department, will evaluate the work. The marks obtained in these two assessments will be combined to get the

final evaluation out of 100 marks. The course grading, like other courses, will be relative in nature.

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 phase-II.

Correlation between COs and POs

PO / CO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6
CO 1	3	3	3	3	2	2
CO 2	3	3	3	2	2	2
CO 3	3	3	3	2	2	2
CO 4	2	3	2	2	2	3
CO 5	2	3	2	2	2	3
CO 6	2	3	2	2	2	3

Detailed Syllabus: Semester IV

[VSEC] Dissertation Phase – II

Teaching Scheme	**Examination Scheme**
Laboratory: 22 hours/week	Theory: CIE: 70 Marks
Self-Study: 12 hours / Week	**ESE: 30 marks**

Course Outcomes

Students will be able to:

1. Achieve proficiency in the languages, tools, libraries, and technologies used in the dissertation work.
2. Apply project planning principles and techniques to ensure effective and efficient project execution.
3. Demonstrate an understanding of the entire lifecycle of a software product or solution.
4. Produce artifacts such as source code, test plans, and test results based on the dissertation work.
5. Write research paper(s) and a thesis in accordance with publication ethics.
6. Exhibit the presentation skills needed to effectively present the work at various platforms.

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 a suitable Scopus indexed conference/in a journal

Deliverables

1. Source 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-Semester evaluation and End-Semester evaluation. In the Mid Semester Examination, the internal guide, along with a Senior Faculty of the department, will evaluate the work. In the End Semester Examination evaluation, the internal guide, along with an external expert (usually from an Industry) will evaluate the work. The marks obtained in these two assessments will be combined to get the final evaluation out of 100 marks. The course grading, like other courses, will be relative in nature.

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-Semester evaluation is also to check preparedness of students for the End-Semester evaluation. Examiners 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, the student may be asked to take an extension in time to complete the course.

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

The total assessment of phase-II work is for 100 marks and the grading, like other courses, will be relative.

Correlation between COs and POs

PO / CO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6
CO 1	3	3	3	3	2	2
CO 2	3	3	3	2	2	2
CO 3	3	3	3	2	2	2
CO 4	2	3	2	2	2	3
CO 5	2	3	2	2	2	3
CO 6	2	3	2	2	2	3