RATHINAM TECHNICAL CAMPUS
(AUTONOMOUS)

A+ ACCREDITED BY NAAC

DEPARTMENT OF BIO METRICS AND CYBER SECURITY

CURRICULUM SYLLABI

(Semesters: I to IV)

Regulation-2022

Programme: M.E. BIOMETRICS AND CYBER SECURITY

2022 Regulations

(2022 Batch onwards)

Curriculum for Semesters I to IV

SEMESTER I

S. No	Course Code	Course	L	T	P	Total Contact Periods/Week	Credits	External / Internal	Category
Theory cum Practical Courses									
1.	22BC101	Data Exploration and Visualization	3	0	2	5	4	60 / 40	PCC
2.	22BC102	Biometric Systems	3	0	2	5	4	60 / 40	PCC
Theory Courses									
3.	22BC103	Advanced Data Structure and Algorithms	3	0	0	3	3	60 / 40	PCC
4.	22FC102	Algebra and Probability	3	1	0	4	4	60 / 40	FC
5.	22RM101	Research Methodology and IPR	2	0	0	2	2	60 / 40	RMC
6.	22BC104	Cyber Forensics and Investigation	3	0	0	3	3	60 / 40	PCC
Practical Course									
7.	22BC105	Advanced Data Structure and Algorithms Laboratory	0	0	4	4	2	40 / 60	PCC

SEMESTER II

S. No	Course Code	Course	L	T	P	Total Contact Periods/Week	Credits	External / Internal	Category
Theory cum Practical Courses									
1.	22BM201	Applied Cryptography	3	0	2	5	4	60 / 40	PCC
2.	22BM202	Machine Learning	3	0	2	5	4	60 / 40	PCC
3.	22BM203	Ethical Hacking	3	0	2	5	4	60 / 40	PCC
Theory Courses									
4.	22BM204	Biometric Data Processing	3	0	0	3	3	60 / 40	PCC
5.		Professional Elective - I	3	0	0	3	3	60 / 40	PEC
6.		Audit Course - I *	2	0	0	2	0	0 / 100	AC
Practical Course									
7.	22BM205	Biometric Data Processing Laboratory	0	0	4	4	2	60 / 40	PCC
8.	22EEC202	Term Paper Writing and Seminar	0	0	2	2	1	0 / 100	EEC

SEMESTER III

S. No	Course Code	Course	L	T	P	Total Contact Periods/Week	Credits	External / Internal	Category
Theory cum Practical Course									
1.		Professional Elective – IV	3	0	2	5	4	60 / 40	PEC
Theory Courses									
2.		Professional Elective – II	3	0	0	3	3	60 / 40	PEC
3.		Professional Elective – III	3	0	0	3	3	60 / 40	PEC
4.		Open Elective	3	0	0	3	3	60 / 40	OEC
5.		Audit Course – II*	2	0	0	2	0	0 / 100	AC

Practical Course									
6.	22EEC301	Project Work I	0	0	12	12	6	60 / 40	EEC

***** Audit Course is optional

SEMESTER IV

S. No	Course Code	Course	L	T	P	Total Contact Periods/Week	Credits	External / Internal	Category
Practical Course									
1.	22EEC401	Project Work II	0	0	24	24	12	60 / 40	EEC

Total Credits: 74

SUMMARY

S.No	SUBJECT AREA	CREDITS AS PER SEMESTER				CREDITS TOTAL
		I	II	III	IV	
1	**FC**	4				**4**
2	**PCC**	16	17			**33**
3	**PEC**		3	10		**13**
4	**RMC**	2				**2**
5	**EEC**		1	6	12	**19**
6	**OEC**			3		**3**
	Total	**22**	**21**	**19**	**12**	**74**
9	**AC**		**~**	**~**		

FOUNDATION COURSES (FC)

S. No	Course Code	Course	L	T	P	Total Contact Periods/Week	Credits	External / Internal	Category
1.	22FC102	Algebra and Probability	3	1	0	4	4	60 / 40	FC

PROFESSIONAL CORE COURSES (PCC)

S. No	Course Code	Course	L	T	P	Total Contact Periods/Week	Credits	External / Internal	Category
1.	22BC101	Data Exploration and Visualization	3	0	2	5	4	60 / 40	PCC
2.	22BC102	Biometric Systems	3	0	2	5	4	60 / 40	PCC
3.	22BC103	Advanced Data Structure and Algorithms	3	0	0	3	3	60 / 40	PCC
4.	22BC104	Cyber Forensics and Investigation	3	0	0	3	3	60 / 40	PCC
5.	22BC105	Advanced Data Structure and Algorithms Laboratory	0	0	4	4	2	40 / 60	PCC
6.	22BM201	Applied Cryptography	3	0	2	5	4	60 / 40	PCC
7.	22BM202	Machine Learning	3	0	2	5	4	60 / 40	PCC
8.	22BM203	Ethical Hacking	3	0	2	5	4	60 / 40	PCC
9.	22BM204	Biometric Data Processing	3	0	0	3	3	60 / 40	PCC
10.	22BM205	Biometric Data Processing Laboratory	0	0	4	4	2	60 / 40	PCC

RESEARCH METHODOLOGY AND IPR COURSE (RMC)

S. No	Course Code	Course	L	T	P	Total Contact Periods/Week	Credits	External / Internal	Category
1.	22RM101	Research Methodology and IPR	2	0	0	2	2	60 / 40	RMC

EMPLOYABILITY ENHANCEMENT COURSES (EEC)

S. No	Course Code	Course	L	T	P	Total Contact Periods/Week	Credits	External / Internal	Category
1.	22EEC202	Term Paper Writing and Seminar	0	0	2	2	1	0 / 100	EEC
2.	22EEC301	Project Work I	0	0	12	12	6	60 / 40	EEC
3.	22EEC401	Project Work II	0	0	24	24	12	60 / 40	EEC

AUDIT COURSES (AC)

S. No	Course Code	Course	L	T	P	Total Contact Periods/Week	Credits	External / Internal	Category
1.	22AC001	English for Research Paper Writing	2	0	0	2	0	0 / 100	AC
2.	22AC002	Disaster Management	2	0	0	2	0	0 / 100	AC
3.	22AC003	Constitution of India	2	0	0	2	0	0 / 100	AC
4.	22AC004	நற்றமிழ் இலக்கியம்	2	0	0	2	0	0 / 100	AC

PROFESSIONAL ELECTIVE COURSES (PEC)

PROFESSIONAL ELECTIVE - I

S. No	Course Code	Course	L	T	P	Total Contact Periods/Week	Credits	External / Internal	Category
1.	22PBM01	Principles of Secure Coding	3	0	0	3	3	60 / 40	PEC
2.	22PBM02	Network Security	3	0	0	3	3	60 / 40	PEC
3.	22PBM03	Public Key Infrastructure	3	0	0	3	3	60 / 40	PEC
4.	22PBM04	Operating Systems Security	3	0	0	3	3	60 / 40	PEC
5.	22PBM05	Security Practices	3	0	0	3	3	60 / 40	PEC
6.	22PBM06	Media Security	3	0	0	3	3	60 / 40	PEC

PROFESSIONAL ELECTIVE - II

S. No	Course Code	Course	L	T	P	Total Contact Periods/Week	Credits	External / Internal	Category
1.	22PBM07	Biometric Security	3	0	0	3	3	60 / 40	PEC
2.	22PBM08	Secure Systems Engineering	3	0	0	3	3	60 / 40	PEC
3.	22PBM09	Cloud Security	3	0	0	3	3	60 / 40	PEC
4.	22PBM10	Firewall and VPN Security	3	0	0	3	3	60 / 40	PEC
5.	22PBM11	Mobile and Digital Forensics	3	0	0	3	3	60 / 40	PEC

PROFESSIONAL ELECTIVE - III

S. No	Course Code	Course	L	T	P	Total Contact Periods/Week	Credits	External / Internal	Category
1.	22PBM12	Access Control and Identity	3	0	0	3	3	60 / 40	PEC

		Management Systems						
2.	22PBM13	Social Network Analysis	3	0	0	3	3	60 / 40	PEC
3.	22PBM14	Data Privacy	3	0	0	3	3	60 / 40	PEC
4.	22PBM15	Security in Cyber-Physical Systems	3	0	0	3	3	60 / 40	PEC
5.	22PBM16	Cryptanalysis	3	0	0	3	3	60 / 40	PEC
6.	22PBM17	Data Analytics for Fraud Detection	3	0	0	3	3	60 / 40	PEC

PROFESSIONAL ELECTIVE - IV

S. No	Course Code	Course	L	T	P	Total Contact Periods/Week	Credits	External / Internal	Category
1.	22PBM18	Internet of Things	3	0	2	5	4	60 / 40	PEC
2.	22PBM19	Malware Analysis	3	0	2	5	4	60 / 40	PEC
3.	22PBM20	Secure Software Design and Development	3	0	2	5	4	60 / 40	PEC
4.	22PBM21	Security Assessment and Risk Analysis	3	0	2	5	4	60 / 40	PEC
5.	22PBM22	Steganography and Digital Watermarking	3	0	2	5	4	60 / 40	PEC
6.	22PBM23	Blockchain Technologies	3	0	2	5	4	60 / 40	PEC
7.	22PBM24	Web Security	3	0	2	5	4	60 / 40	PEC

OPEN ELECTIVE COURSES (OEC)

S. No	Course Code	Course	L	T	P	Total Contact Periods/Week	Credits	External / Internal	Category
1.	22OAE01	Big Data Analytics	3	0	0	3	3	60 / 40	OEC
2.	22OAE02	Internet of Things and Cloud	3	0	0	3	3	60 / 40	OEC
3.	22OAE03	Medical Robotics	3	0	0	3	3	60 / 40	OEC
4.	22OAE04	Embedded Automation	3	0	0	3	3	60 / 40	OEC

22BC101	DATA EXPLORATION AND VISUALIZATION	L	T	P	C
		3	0	2	4

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. To outline an overview of exploratory data analysis.
2. To implement data visualization using Matplotlib.
3. To perform univariate data exploration and analysis.
4. To apply bivariate data exploration and analysis.
5. To use Data exploration and visualization techniques for multivariate and time series data

Course Content:

UNIT I EXPLORATORY DATA ANALYSIS 9

EDA fundamentals – Understanding data science – Significance of EDA – Making sense of data –Comparing EDA with classical and Bayesian analysis – Software tools for EDA - Visual Aids forEDA- Data transformation techniques-merging database, reshaping and pivoting, Transformation techniques - Grouping Datasets - data aggregation – Pivot tables and cross-tabulations

UNIT II VISUALIZING USING MATPLOTLIB 9

Importing Matplotlib – Simple line plots – Simple scatter plots – visualizing errors – density and contour plots – Histograms – legends – colors – subplots – text and annotation – customization– three-dimensional plotting - Geographic Data with Basemap - Visualization with Seaborn.

UNIT III UNIVARIATE ANALYSIS 9

Introduction to Single variable: Distributions and Variables - Numerical Summaries of Level andSpread - Scaling and Standardizing – Inequality - Smoothing Time Series

UNIT IV BIVARIATE ANALYSIS 9

Relationships between Two Variables - Percentage Tables - Analyzing Contingency Tables - Handling Several Batches - Scatterplots and Resistant Lines – Transformations.

UNIT V MULTIVARIATE AND TIME SERIES ANALYSIS 9

Introducing a Third Variable - Causal Explanations - Three-Variable Contingency Tables andBeyond - Longitudinal Data – Fundamentals of TSA – Characteristics of time series data – DataCleaning – Time-based indexing – Visualizing – Grouping – Resampling

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Understand the fundamentals of exploratory data analysis.

2. Implement the data visualization using Matplotlib.
3. Perform univariate data exploration and analysis.
4. Apply bivariate data exploration and analysis.
5. Use Data exploration and visualization techniques for multivariate and time series data that will help enhance the cyber security

Text Book(s):

1. Suresh Kumar Mukhiya, Usman Ahmed, “Hands-On Exploratory Data Analysis with Python”, Packt Publishing, 2020. (Unit 1)
2. Jake Vander Plas, "Python Data Science Handbook: Essential Tools for Working with Data", Oreilly, 1st Edition, 2016. (Unit 2)
3. Catherine Marsh, Jane Elliott, “Exploring Data: An Introduction to Data Analysis for Social Scientists”, Wiley Publications, 2nd Edition, 2008. (Unit 3,4,5)

Reference Books:

1. Eric Pimpler, Data Visualization and Exploration with R, GeoSpatial Training service,
2. 2017.
3. Claus O. Wilke, “Fundamentals of Data Visualization”, O’reilly publications, 2019.
4. Matthew O. Ward, Georges Grinstein, Daniel Keim, “Interactive Data Visualization:
5. Foundations, Techniques, and Applications”, 2nd Edition, CRC press, 2015

List of Experiments:

1. Perform exploratory data analysis (EDA) on with datasets like email data set .Export all your emails as a dataset, import them inside a pandas data frame, visualize them and get different insights from the data **3**
2. Explore various variable and row filters in R for cleaning data. Apply various plot features in R on sample data sets and visualize. 3
3. Perform Data Analysis and representation on a Map using various Map data sets with Mouse Rollover effect, user interaction, etc.. 3
4. Build cartographic visualization for multiple datasets involving various countries of the world; states and districts in India etc. 3
5. Use a case study on a data set and apply the various EDA and visualization techniques and present an analysis report. 3

TOTAL PRACTICAL PERIODS 15 Periods

TOTAL LECTURE CUM PRACTICAL PERIODS 60 Periods

List of Equipments: (for batch of 30 students)

1. Systems with Linux Operating System with gnu compiler 30 nos

22BC102	BIOMETRIC SYSTEMS	L	T	P	C
		3	0	2	4

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. To learn and understand biometric technologies and their functionalities.
2. To learn the role of biometric in the organization
3. To learn the computational methods involved in the biometric systems.
4. To expose the context of Biometric Applications
5. To learn to develop applications with biometric security

Course Content:

UNIT I INTRODUCTION 9+3

Introduction – history – type of biometrics – General architecture of biometric systems – Basic working of biometric matching – Biometric system error and performance measures – Design of biometric systems – Applications of biometrics – Biometrics versus traditional authentication methods – character recognition – authentication technologies, biometric technologies, Finger, face, voice and iris biometric technologies.

UNIT II FINGERPRINT, FACE AND IRIS AS BIOMETRICS 9+3

Fingerprint biometrics – Fingerprint recognition system – Minutiae extraction – Fingerprint indexing– experimental results – Biometrics using vein pattern of palm – Advantages and disadvantages – Basics of hand geometry

Background of face recognition – Design of face recognition system – Neural network for face recognition – Face detection in video sequences – Challenges in face biometrics – Face recognition methods – Advantages and disadvantages

Iris segmentation method – Determination of iris region – Experimental results of iris localization –applications of iris biometrics – Advantages and disadvantages.

UNIT III PRIVACY ENHANCEMENT AND MULTIMODAL BIOMETRICS 9+3

Privacy concerns associated with biometric developments – Identity and privacy – Privacy concerns – biometrics with privacy enhancement – Comparison of various biometrics in terms of privacy – Soft biometrics - Introduction to biometric cryptography – General purpose cryptosystem – Modern cryptography and attacks – Symmetric key ciphers – Cryptographic algorithms – Introduction to multimodal biometrics – Basic architecture using face and ear – Characteristics and advantages of multimodal biometrics characters – AADHAAR : An Application of Multimodal Biometrics.

UNIT IV WATERMARKING TECHNIQUES & BIOMETRICS: SCOPE AND FUTURE 9+3

Data hiding methods – Basic framework of watermarking – Classification, Applications, Attacks, Performance Evaluation and Characteristics – General Watermarking process – Image watermarking techniques – Watermarking algorithm – Effect of attacks on watermarking techniques –Scope and future market of biometrics

Applications of Biometrics and information technology infrastructure – Role of biometrics in enterprise security – Role of biometrics in border security – Smart card technology and biometric – Radio frequency identification biometrics – DNA Biometrics – Comparative study of various biometrics techniques.

UNIT V IMAGE ENHANCEMENT TECHNIQUES & BIOMETRICS STANDARDS 9+3

Current research in image enhancement techniques – Image enhancement algorithms– Frequency domain filters – Databases and implementation – Standard development organizations – Application programming interface – Information security and biometric standards – Biometric template interoperability biometrics for network security and biometrics for transaction.

TOTAL LECTURE PERIODS 75 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Identify the various biometric technologies.
2. Design of biometric recognition for the organization.
3. Develop simple applications for privacy.
4. Understand the need of biometric in the society.
5. Understand the research in biometric techniques.

Text Book(s):

1. Khalid Saeed, “New Directions in Behavioral Biometrics', CRC Press 2020.
2. John D Woodward, Jr.; Nicholas M Orlans; Peter T Higgins, Biometrics – The Ultimate Reference, Wiley Dreamtech.College Publications, 2015.

Reference Books:

1. G R Sinha and Sandeep B. Patil, Biometrics: Concepts and Applications, Wiley, 2013
2. Paul Reid, Biometrics for Network Security, Pearson Education, 2003
3. Samir Nanavathi, Micheal Thieme, Raj Nanavathi, Biometrics – Identity verification in a networked world, Wiley – dream Tech, 2002.
4. Rafael C. Gonzalez, Richard Eugene Woods, Digital Image Processing using MATLAB, 2nd Edition, Tata McGraw-Hill Education 2010.
5. Ruud M. Bolle, Sharath Pankanti, Nalini K. Ratha, Andrew W. Senior, Jonathan H. Connell, Guide to Biometrics, Springer 2009.

List of Experiments:

1.	Student school smart card	**3**
2.	Secure lab access using card scanner plus face recognition	**3**
3.	Student bus pass with barcode card scan	**3**
4.	Student bus pass with webcam scan	**3**
5.	Employee attendance system by Qr scan	**3**
6.	Student examination datacard	**3**
7.	School student attendance system by barcode scan	**3**
8.	School student attendance system by Qr scan	**3**
9.	School student attendance with fingerprint reader	**3**
10.	Fingerprint voting system project	**3**

TOTAL PRACTICAL PERIODS 30 Periods

TOTAL LECTURE CUM PRACTICAL PERIODS 75 Periods

List of Equipments: (for batch of 30 students)

1.	INTEL based desktop PC with min. 8GB RAM and 500 GB HDD, 17” or higher TFT Monitor, Keyboard and mouse and GPU as required	30 nos
2.	Windows 10 or higher operating system / Linux Ubuntu 20 or higher	30 nos
3.	OpenBR / OpenFace Tracker/Open EBTS/Insight Face	30 nos
4.	Kairos API/Face++/Crypto++ Python 3.9 or higher	30 nos

22BC103	ADVANCED DATA STRUCTURES AND ALGORITHMS	L	T	P	C
		3	0	0	3

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. To understand the usage of algorithms in computing
2. To learn and use hierarchical data structures and its operations
3. To learn the usage of graphs and its applications
4. To select and design data structures and algorithms that is appropriate for problems
5. To study about NP Completeness of problems.

Course Content:

UNIT I ROLE OF ALGORITHMS IN COMPUTING & COMPLEXITY ANALYSIS 9

Algorithms – Algorithms as a Technology -Time and Space complexity of algorithms- Asymptotic analysis-Average and worst-case analysis-Asymptotic notation-Importance of efficient algorithms-Program performance measurement - Recurrences: The Substitution Method – The Recursion- Tree Method- Data structures and algorithms.

UNIT II HIERARCHICAL DATA STRUCTURES 9

Binary Search Trees: Basics – Querying a Binary search tree – Insertion and Deletion- Red Black trees: Properties of Red-Black Trees – Rotations – Insertion – Deletion -B-Trees: Definition of B - trees – Basic operations on B-Trees – Deleting a key from a B-Tree- Heap – Heap Implementation– Disjoint Sets - Fibonacci Heaps: structure – Mergeable-heap operations- Decreasing a key and deleting a node-Bounding the maximum degree.

UNIT III GRAPHS 9

Elementary Graph Algorithms: Representations of Graphs – Breadth-First Search – Depth-First Search – Topological Sort – Strongly Connected Components- Minimum Spanning Trees: Growing a Minimum Spanning Tree – Kruskal and Prim- Single-Source Shortest Paths: The Bellman-Ford algorithm – Single-Source Shortest paths in Directed Acyclic Graphs – Dijkstra‘s Algorithm; Dynamic Programming - All-Pairs Shortest Paths: Shortest Paths and Matrix Multiplication – The Floyd-Warshall Algorithm.

UNIT IV ALGORITHM DESIGN TECHNIQUES 9

Dynamic Programming: Matrix-Chain Multiplication – Elements of Dynamic Programming – Longest Common Subsequence- Greedy Algorithms: – Elements of the Greedy Strategy- An Activity-Selection Problem - Huffman Coding.

UNIT V NP COMPLETE AND NP HARD 9

NP-Completeness: Polynomial Time – Polynomial-Time Verification – NP- Completeness and Reducibility – NP-Completeness Proofs – NP-Complete Problems.

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Design data structures and algorithms to solve computing problems.
2. Choose and implement efficient data structures and apply them to solve problems.
3. Design algorithms using graph structure and various string-matching algorithms to solve real-life problems.
4. Design one’s own algorithm for an unknown problem.
5. Apply suitable design strategy for problem solving.

Text Book(s):

1. S.Sridhar,” Design and Analysis of Algorithms”, Oxford University Press, 1st Edition, 2014.
2. Adam Drozdex, “Data Structures and algorithms in C++”, Cengage Learning, 4th Edition, 2013.
3. T.H. Cormen, C.E.Leiserson, R.L. Rivest and C.Stein, "Introduction to Algorithms", Prentice Hall of India, 3rd Edition, 2012.

Reference Books:

1. Mark Allen Weiss, “Data Structures and Algorithms in C++”, Pearson Education, 3rd Edition, 2009.

2. E. Horowitz, S. Sahni and S. Rajasekaran, “Fundamentals of Computer Algorithms”, University Press, 2nd Edition, 2008.
3. Alfred V. Aho, John E. Hopcroft, Jeffrey D. Ullman, “Data Structures and Algorithms”, Pearson Education, Reprint 2006.

22FC102	ALGEBRA AND PROBABILITY	L	T	P	C
		3	1	0	4

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. To understand the basics of random variables with emphasis on the standard discrete and continuous distributions.
2. To make students understand the notion of a Markov chain, and how simple ideas of conditional probability and matrices can be used to give a thorough and effective account of discrete – time Markov chains.
3. To apply the small / large sample tests through Tests of hypothesis.
4. To introduce the basic notions of groups, rings, fields which will then be used to solve related problems.
5. To introduce and apply the concepts of rings, finite fields and polynomials.

Course Content:

UNIT I RANDOM VARIABLES 12

Random variables – Moments – Binomial, Biometric, Poisson, Uniform, Exponential and Normal distributions – Joint distributions – Marginal – Correlation – Linear Regression distributions.

UNIT II RANDOM PROCESSES 12

Classification – Stationary random process – Markov process – Markov chain – Poisson process – Gaussian process – Autocorrelation – Cross correlation.

UNIT III TESTING OF HYPOTHESIS 12

Sampling distributions – Type I and Type II errors – Small and large samples – Tests based on Normal, t, Chi square and F distributions for testing of mean, variance and proportions, Tests for independence of attributes and goodness of fit.

UNIT IV GROUPS AND RINGS 12

Groups: Definition – Properties – Homomorphism - Isomorphism – Cyclic groups – Cosets – Lagrange’s theorem.

Rings: Definition – Sub rings – Integral domain – Field – Integer modulo n – Ring homomorphism.

UNIT V FINITE FIELDS AND POLYNOMIALS 12

Rings – Polynomial rings - Irreducible polynomials over finite fields - Factorizations of polynomials over finite fields.

TOTAL LECTURE PERIODS 60 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Analyze the performance in terms of probabilities and distributions achieved by the determined solutions.
2. Classify various random processes and solve problems involving stochastic processes.
3. Apply the basic principles underlying statistical inference (estimation and hypothesis testing).
4. Apply the basic notions of groups, rings, fields which will then be used to solve related problems.
5. Explain the fundamental concepts of advanced algebra and their role in modern mathematics and applied contexts.

Text Book(s):

1. Devore J.L.,” Probability and Statistics for Engineering and sciences”, Cengage learning, 9th Edition, Boston, 2017.
2. Johnson R. A. and Gupta C.B., “Miller and Freund’s Probability and Statistics for Engineers”, Pearson India Education, Asia, 9th Edition, New Delhi, 2017.

Reference Books:

1. Grimaldi R. P. and Ramana B.V., “Discrete and Combinatorial Mathematics”, Pearson Education, 5th Edition, New Delhi, 2007.
2. Ibe. O.C., “Fundamentals of Applied Probability and Random Processes”, Elsevier U.P., 1st Indian Reprint, 2007.

22RM101	RESEARCH METHODOLOGY AND IPR	L	T	P	C
		2	0	0	2

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. To impart knowledge on formulation of research problem, research methodology, and ethics involved in doing research and importance of IPR protection.

Course Content:

UNIT I RESEARCH DESIGN 6

Overview of research process and design, Use of Secondary and exploratory data to answer the research question, Qualitative research, Observation studies, Experiments and Surveys.

UNIT II DATA COLLECTION AND SOURCES 6

Measurements, Measurement Scales, Questionnaires and Instruments, Sampling and methods.

Data - Preparing, Exploring, examining and displaying.

UNIT III DATA ANALYSIS AND REPORTING 6

Overview of Multivariate analysis, Hypotheses testing and Measures of Association.

Presenting Insights and findings using written reports and oral presentation

UNIT IV INTELLECTUAL PROPERTY RIGHTS 6

Number systems (Binary, Gray, Decimal and Hexa-decimal), Code Converters (Binary to Gray, Gray to Binary, BCD to Excess-3, Excess-3 to BCD) - Combinational logic - representation of logic functions-SOP and POS forms, K-map representations - minimization using K maps-Flip Flops-LogicFamilies(RTL,TTL,CMOS)

UNIT V PATENTS 6

Patents – objectives and benefits of patent, Concept, features of patent, Inventive step, Specification, Types of patent application, process E-filing, Examination of patent, Grant of patent, Revocation, Equitable Assignments, Licences, Licensing of related patents, patent agents, Registration of patent agents.

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Understand that today’s world is controlled by Computer, Information Technology, but tomorrow world will be ruled by ideas, concept, and creativity.
2. Understand research problem formulation & Analyze research related information and Follow research ethics.
3. Correlate the results of any research article with other published results. Write a review article in the field of engineering.
4. Appreciate the importance of IPR and protect their intellectual property. Understand that IPR protection provides an incentive to inventors for further research work and investment in R &

D, which leads to creation of new and better products, and in turn brings about, economic growth and social benefits

Text Book(s):

1. The Institute of Company Secretaries of India, Statutory body under an Act of parliament, “Professional Programme Intellectual Property Rights, Law and practice”, September 2013.
2. Cooper Donald R, Schindler Pamela S and Sharma JK, “Business Research Methods”, Tata McGraw Hill Education, 11e (2012).

Reference Books:

1. Catherine J. Holland, “Intellectual property: Patents, Trademarks, Copyrights, Trade Secrets”, Entrepreneur Press, 2007.
2. David Hunt, Long Nguyen, Matthew Rodgers, “Patent searching: tools & techniques”, Wiley, 2007.

Web Links:

1. https://nptel.ac.in/courses/106105077

22BC104	CYBER FORENSICS AND INVESTIGATION	L	T	P	C
		3	0	0	3

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. To gain a comprehensive understanding of cyber forensic principles and the collection, preservation, and analysis of digital evidence
2. To combine both the technical expertise and the knowledge required to investigate, detect and prevent digital crimes.
3. To understand the different applications and methods for conducting network and digital forensic acquisition and analysis
4. To learn the E-evidence collection and preservation, investigating operating systems and file systems, network, cloud and mobile device forensics
5. To gain knowledge on digital forensics legislations, digital crime, forensic processes and procedures.

Course Content:

UNIT I CYBER FORENSICS SCIENCE 9

Cyber Forensics Science: Forensics Science, Forensics Fundamentals, Computer Forensics, and Digital Forensics.

Cyber Crime: Criminalistics as it relates to the Investigative Process, Analysis of Cyber Criminalistics Area, Holistic Approach to Cyber-forensics, Computer Forensics and Law Enforcement- Indian Cyber Forensic - Forensics Services, Professional Forensics Methodology- Types of Forensics Technology

UNIT II NETWORK SECURITY FORENSICS SYSTEM AND SERVICES 9

Forensics system and Services : Forensics on - Internet Usage – Intrusion - Firewall and Storage Area Network; Occurrence of Cyber-crimes- Cyber Detectives- Fighting Cyber Crimes- Forensic Process

Open-source Security Tools for Network Forensic Analysis, Requirements for Preservation of Network Data

Computer Forensics - Data Backup and Recovery - Test Disk Suite.

UNIT III DIGITAL FORENSICS PRESERVATION AND FORENSIC DATA ANALYSIS 9

Digital Repositories - Evidence Collection – Data Preservation Approaches – Meta Data and Historic records – Legal aspects. Basic Steps of Forensic Analysis in Windows and Linux – Forensic Scenario – Email Analysis – File Signature Analysis – Hash Analysis – Forensic Examination of log files

Data-Recovery Solution, Hiding and Recovering Hidden Data, Evidence Collection and Data Seizure.

UNIT IV CLOUD, NETWORK AND MOBILE FORENSICS 9

Working with the cloud vendor, obtaining evidence, reviewing logs and APIs Mobile Forensics techniques, Mobile Forensics Tools - Android Device – Analysis- Android Malware – iOS Forensic Analysis – SIM Forensic Analysis – Case study

Recent trends in Mobile Forensic Technique and methods to Search and Seize Electronic Evidence

UNIT V LEGAL ASPECTS OF DIGITAL FORENSICS 9

IT Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT IPC and CrPC , Electronic Communication Privacy ACT, Legal Policies, Act 2000,

Amendment of IT Act 2008.

Current Cyber Forensic Tools: Overview of different software packages – Encase-Autopsy-Magnet – Wireshark - Mobile Forensic Tools – SQLite

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Understand the responsibilities and liabilities of a computer forensic investigator
2. Identify potential sources of electronic evidence.
3. Understand the importance of maintaining the integrity of digital evidence.
4. Demonstrate the ability to perform basic forensic data acquisition and analysis using computer and network based applications and utilities.
5. Understand relevant legislation and codes of ethics.

Text Book(s):

1. J. R. Vacca, Computer forensics: Computer Crime Scene investigation, 2nd Ed. Hanover, NH, United States: Charles River Media, 2002, Laxmi Publications, 1st Edition, 2015.
2. Nelson, Phillips and Enfinger Steuart, “Guide to Computer Forensics and Investigations”, 6th Edition, Cengage Learning, New Delhi, 2020.
3. C. Altheide, H. Carvey, and R. Davidson, Digital Forensics with Open Source Tools: Using Open Source Platform Tools for Performing Computer Forensics on Target Systems: Windows, Mac, Linux, Unix, etc, 1st Ed. United States: Syngress, 2011.

Reference Books:

1. S. Bommisetty, R. Tamma, and H. Mahalik, Practical Mobile Forensics: Dive into Mobile Forensics on IOS, Android, Windows, and blackBerry devices with this action-packed, practical guide. United Kingdom: Packt Publishing, 2014.
2. G. Gogolin, Digital Forensics Explained, 1st Ed. Boca Raton, FL: CRC Taylor & Francis, 1st Edition, Auerbach Publications, 2013.
3. Hoog and J. McCash, Android forensics: Investigation, Analysis, and Mobile Security for Google Android. Waltham, MA: Syngress Media, U.S., 2011.
4. B. Nelson, A. Phillips, F. Enfinger, and C. Steuart, Guide to Computer Forensics and Investigations, Second edition, 2nd Ed. Boston: Thomson Course Technology, 2009.
5. C. Altheide and H. Carvey, “Digital Forensics with Open Source Tools”, 2011 Publisher(s): Syngress.

6. J. Sammons, “The Basics of Digital Forensics- The Primer for Getting Started in Digital Forensics”, 1st Edition, Syngress, 2012.

22BC105	**ADVANCED DATA STRUCTURES AND ALGORITHMS LABORATORY**	**L**	**T**	**P**	**C**
		0	**0**	**4**	**2**

Pre-requisite **Syllabus Version** V 0.1

List of Experiments:

1.	Implementation of recursive function for tree traversal and Fibonacci	**5**
2.	Implementation of iteration function for tree traversal and Fibonacci	**5**
3.	Implementation of Merge Sort and Quick Sort	**5**
4.	Implementation of a Binary Search Tree	**5**
5.	Red-Black Tree Implementation	**5**
6.	Heap Implementation	**5**
7.	Fibonacci Heap Implementation	**5**
8.	Graph Traversals	**5**
9.	Spanning Tree Implementation	**5**
10.	Shortest Path Algorithms (Dijkstra's algorithm, Bellman Ford Algorithm)	**5**
11.	Implementation of Matrix Chain Multiplication	**5**
12.	Activity Selection and Huffman Coding Implementation	**5**
	TOTAL PRACTICAL PERIODS	**60 Periods**

Expected Course Outcome: On completion of the course, the student is expected to

1. To acquire the knowledge of using advanced tree structures
2. To learn the usage of heap structures
3. To understand the usage of graph structures and spanning trees
4. To understand the problems such as matrix chain multiplication, activity selection and Huffman coding
5. To understand the necessary mathematical abstraction to solve problems.

Reference Books:

1. Lipschutz Seymour, “Data Structures Schaum's Outlines Series”, Tata McGraw Hill, 3rd Edition, 2014.
2. Alfred V. Aho, John E. Hopcroft, Jeffrey D. Ullman, “Data Structures and Algorithms”, Pearson Education, Reprint 2006.
3. http://www.coursera.org/specializations/data-structures-algorithms
4. http://www.tutorialspoint.com/data_structures_algorithms
5. http://www.geeksforgeeks.org/data-structures/

List of Equipments: (for batch of 30 students)

1.	64-bit Open source Linux or its derivative	30 no
2.	Open Source C++ Programming tool like G++/GCC	30 no

22BM201	Applied Cryptography	L	T	P	C
		3	0	2	4

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. To understand OSI security architecture and classical encryption techniques.
2. To acquire fundamental knowledge on the concepts of finite fields and number theory.
3. Understand various block cipher and stream cipher models.
4. Describe the principles of public key cryptosystems, hash functions and digital signature
5. Acquire fundamental knowledge on applications of Digital Signature in payments etc.,

Course Content:

UNIT I MATHEMATICAL FOUNDATION AND NUMBER THEORY 10

Definitions – Cryptography, cryptanalysis, cryptology, classical cryptosystem- shift cipher, affine cipher, vigenere cipher, substitution, transposition techniques, Types of attacks in OSI security architecture-Number Theory concepts – Modular Arithmetic , Properties, Euclidean algorithm, Fermat's and Euler's theorem, Chinese Remainder Theorem, Primitive roots, Discrete Logarithms, Computational aspects, finite fields, Primes and unique factorization of integers, Computing discrete logarithms

UNIT II BLOCK CIPHERS AND MODES OF OPERATIONS 8

Simplified DES - Data Encryption Standard-Block cipher principles-block cipher modes of operationAES-TripleDES-Blowfish-RC5

UNIT III PUBLIC KEY CRYPTOGRAPHY 8

Principles and characteristics - Need for public key cryptography - Primality Testing - Miller Rabin Test - Diffie Hellman Key Exchange-MITM Attack - RSA, Fast Modular Exponentiation Algorithms, RandomNumberGeneration – FiniteFields–PolynomialArithmetic-ECC – KeyManagement

UNIT IV HASH FUNCTIONS AND DIGITAL SIGNATURE 9

Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC – MD5 - SHA - HMAC – CMAC - Digital signature and authentication protocols – DSS – EI Gamal – Schnorr - Blind Signatures for unreachable payments

UNIT V APPLICATIONS OF CRYPTOGRAPHIC ALGORITHMS 10

Authentication – Kerberos , Zero Knowledge Proofs, System Security - Firewalls, Types, Design considerations, Intrusion Detection Systems, IP Security - IPSec (AH and ESP),Web Security - SSL, TLS, Electronic passports and ID cards - SDA/DDA/CDA Bank Cards,Secure Electronic Transaction,Crypto currencies - Bitcoin, Email Security - PGP, Tor (The Onion Router).

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Compare various Cryptographic Techniques
2. Understand security issues, practices and principles in various applications
3. Learn to analyse the security of the in-built cryptosystems
4. Develop cryptographic algorithms for information security
5. Develop authentication schemes for identity and membership authorization

Text Book(s):

1. Bruce Schneier and Neils Ferguson, “Practical Cryptography”, First Edition, Wiley Dreamtech India Pvt Ltd, 2003.
2. J. H. Silverman, A Friendly Introduction to Number Theory, 4th Ed. Boston: Pearson, 2019 (ISBN No.: 978 9353433079, 935343307X

Reference Books:

1. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security : Private Communications in a Public World”, Prentice Hall of India, Second Edition, 2016. (UNIT V)
2. Douglas R Stinson and Maura B. Paterson, “Cryptography – Theory and practice”, Fourth Edition, CRC Press,2018 (UNIT -I)
3. William Stallings, Cryptography and Network Security, Seventh Edition, Pearson Education, 2017. (UNIT I,II,III,IV)

List of Experiments:

1.	Demonstration of Symmetric conventional cryptographic techniques	**3**
2.	Demonstration of Symmetric classic cryptographic techniques	**3**
3.	Demonstration of Asymmetric cryptographic techniques.	**3**
4.	Demonstration of Hashing and Message digest techniques	**3**
5.	Design and implementation of new cryptographic algorithms	**3**
6.	Demonstration and Implementation of secure communication using standard crypto libraries (OpenSSL, NTL, GMP)	**3**
7.	Implementation of smart card based server/client applications.	**3**
8.	Demonstration of authentication techniques	**3**
9.	Developing cryptographic algorithms for industrial applications.	**3**
10.	Developing cryptographic algorithms for innovative applications.	**3**

TOTAL PRACTICAL PERIODS 30 Periods

TOTAL LECTURE CUM PRACTICAL PERIODS 75 Periods

22BM202	**MACHINE LEARNING**	**L**	**T**	**P**	**C**
		3	**0**	**2**	**4**

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. To understand the concepts and mathematical foundations of machine learning and types of problems tackled by machine learning
2. To explore the different supervised learning techniques including ensemble methods To learn different aspects of unsupervised learning and reinforcement learning
3. To learn the role of probabilistic methods for machine learning
4. To understand the basic concepts of neural networks and deep learning

Course Content:

UNIT I INTRODUCTION AND MATHEMATICAL FOUNDATIONS 9

What is Machine Learning? Need –History – Definitions – Applications - Advantages, Disadvantages & Challenges -Types of Machine Learning Problems – Mathematical Foundations - Linear Algebra & Analytical Geometry -Probability and Statistics- Bayesian Conditional Probability -Vector Calculus & Optimization - Decision Theory - Information theory

UNIT II SUPERVISED LEARNING 9

Introduction-Discriminative and Generative Models -Linear Regression - Least Squares - Under-fitting / Overfitting -Cross-Validation – Lasso Regression- Classification - Logistic Regression- Gradient Linear Models -Support Vector Machines –Kernel Methods -Instance based Methods - K-Nearest Neighbours - Tree based Methods –Decision Trees –ID3 – CART - Ensemble Methods –Random Forest - Evaluation of Classification Algorithms

UNIT III UNSUPERVISED LEARNING AND REINFORCEMENT LEARNING 9

Introduction - Clustering Algorithms -K – Means – Hierarchical Clustering - Cluster Validity - Dimensionality Reduction –Principal Component Analysis – Recommendation Systems - EM algorithm. Reinforcement Learning – Elements -Model based Learning – Temporal Difference Learning

UNIT IV PROBABILISTIC METHODS FOR LEARNING- 9

Introduction -Naïve Bayes Algorithm -Maximum Likelihood -Maximum Apriori -Bayesian Belief Networks -Probabilistic Modelling of Problems -Inference in Bayesian Belief Networks – Probability Density Estimation - Sequence Models – Markov Models – Hidden Markov Models

UNIT V NEURAL NETWORKS AND DEEP LEARNING 9

Neural Networks – Biological Motivation- Perceptron – Multi-layer Perceptron – Feed Forward Network – Back Propagation-Activation and Loss Functions- Limitations of Machine Learning – Deep Learning– Convolution Neural Networks – Recurrent Neural Networks – Use cases

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Understand and outline problems for each type of machine learning
2. Design a Decision tree and Random forest for an application
3. Implement Probabilistic Discriminative and Generative algorithms for an application and analyze the results.
4. Use a tool to implement typical Clustering algorithms for different types of applications.
5. Design and implement an HMM for a Sequence Model type of application and identify applications suitable for different types of Machine Learning with suitable justification.

Text Book(s):

1. Aurélien Géron , Hands-On Machine Learning with Scikit-Learn and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems 2nd Edition, o'reilly, (2017)
2. Hal Daumé III, “A Course in Machine Learning”, 2017 (freely available online).

Reference Books:

1. Stephen Marsland, “Machine Learning: An Algorithmic Perspective”, Chapman & Hall/CRC, 2nd Edition, 2014.
2. Kevin Murphy, “Machine Learning: A Probabilistic Perspective”, MIT Press, 2012
3. Ethem Alpaydin, “Introduction to Machine Learning”, Third Edition, Adaptive Computation and Machine Learning Series, MIT Press, 2014
4. Tom M Mitchell, “Machine Learning”, McGraw Hill Education, 2013.
5. Peter Flach, “Machine Learning: The Art and Science of Algorithms that Make Sense of Data”, First Edition, Cambridge University Press, 2012.
6. Shai Shalev-Shwartz and Shai Ben-David, “Understanding Machine Learning: From Theory to Algorithms”, Cambridge University Press, 2015
7. Christopher Bishop, “Pattern Recognition and Machine Learning”, Springer, 2007.

List of Experiments:

1. Implement a Linear Regression with a Real Dataset (https://www.kaggle.com/harrywang/housing). Experiment with different features in building a model. Tune the model's hyperparameters. **3**
2. Implement a binary classification model. That is, answers a binary question such as "Are houses in this neighborhood above a certain price?"(use data from exercise 1). Modify the classification threshold and determine how that modification influences the model. Experiment with different classification metrics to determine your model's effectiveness. **3**
3. Classification with Nearest Neighbours. In this question, you will use the scikit-learn’s KNN classifer to classify real vs. fake news headlines. The aim of this question is for you to read the scikitlearn API and get comfortable with training/validation splits. Use California Housing Dataset **3**
4. In this exercise, you'll experiment with validation sets and test sets using the dataset. Split a training set into a smaller training set and a **3**

validation set. Analyze deltas between training set and validation set results. Test the trained model with a test set to determine whether your trained model is overfitting. Detect and fix a common training problem.

5. Implement the k-means algorithm using https://archive.ics.uci.edu/ml/datasets/Codon+usage dataset **3**

6. Implement the Naïve Bayes Classifier using https://archive.ics.uci.edu/ml/datasets/Gait+Classification dataset **3**

7. Project - (in Pairs) Your project must implement one or more machine learning algorithms and apply them to some data. a. Your project may be a comparison of several existing algorithms, or it may propose a new algorithm in which case you still must compare it to at least one other approach. b. You can either pick a project of your own design, or you can choose from the set of predefined projects. c. You are free to use any third-party ideas or code that you wish as long as it is publicly available. d. You must properly provide references to any work that is not your own in the write-up. e. Project proposal You must turn in a brief project proposal. Your project proposal should describe the idea behind your project. You should also briefly describe software you will need to write, and papers (2-3) you plan to read. **3**

8. List of Projects (datasets available) **3**
    1. Sentiment Analysis of Product Reviews
    2. Stock Prediction 20
    3. Sales Forecasting
    4. Music Recommendation
    5. Handwriting Digit Classification
    6. Fake News Detection
    7. Sports Prediction
    8. Object Detection
    9. Disease Prediction

TOTAL PRACTICAL PERIODS 30 Periods

TOTAL LECTURE CUM PRACTICAL PERIODS 75 Periods

22BM203	ETHICAL HACKING	L	T	P	C
		3	0	2	4

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. To understand and analyze security threats & countermeasures related to ethical hacking.
2. To learn the different levels of vulnerabilities at a system level.
3. To gain knowledge on the different hacking methods for web services and session hijacking.
4. To understand the hacking mechanisms on how a wireless network is hacked.

Course Content:

UNIT I ETHICAL HACKING OVERVIEW & VULNERABILITIES 9

Understanding the importance of security, Concept of ethical hacking and essential Terminologies- Threat, Attack, Vulnerabilities, Target of Evaluation, Exploit. Phases involved in hacking

UNIT II FOOTPRINTING & PORT SCANNING 9

Footprinting - Introduction to foot printing, Understanding the information gathering methodology ofthe hackers, Tools used for the reconnaissance phase, Port Scanning - Introduction, using port scanning tools, ping sweeps, Scripting Enumeration-Introduction, Enumerating windows OS & LinuxOS

UNIT III SYSTEM HACKING 9

Aspect of remote password guessing, Role of eavesdropping ,Various methods of password cracking, Keystroke Loggers, Understanding Sniffers ,Comprehending Active and Passive Sniffing, ARP Spoofing and Redirection, DNS and IP Sniffing, HTTPS Sniffing.

UNIT IV HACKING WEB SERVICES & SESSION HIJACKING 9

Web application vulnerabilities, application coding errors, SQL injection into Back-end Databases, cross-site scripting, cross-site request forging, authentication bypass, web services and related flaws, protective http headers. Understanding Session Hijacking, Phases involved in Session Hijacking,Types of Session Hijacking, Session Hijacking Tools

UNIT V HACKING WIRELESS NETWORKS 9

Introduction To 802.11, Role Of WEP, Cracking WEP Keys, Sniffing Traffic, Wireless DOS Attacks, Wlanscanners, Wlansniffers,Hackingtools,Securing Wireless Network

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Understand vulnerabilities, mechanisms to identify vulnerabilities/threats/attacks
2. Use tools to identify vulnerable entry points
3. Identify vulnerabilities using sniffers at different layers
4. Handle web application vulnerabilities
5. Identify attacks in wireless networks

Text Book(s):

1. Kimberly Graves, "Certified Ethical Hacker", Wiley India Pvt Ltd, 2010
2. Michael T. Simpson, "Hands-on Ethical Hacking & Network Defense", Course Technology,
   2010

Reference Books:

1. RajatKhare, "Network Security and Ethical Hacking", Luniver Press, 2006
2. Ramachandran V, "BackTrack 5 Wireless Penetration Testing Beginner's Guide (3rd ed.)."
3. Packt Publishing, 2011
4. Thomas Mathew, "Ethical Hacking", OSB publishers, 2003
5. Matthew Hickey, Jennifer Arcuri, "Hands on Hacking: Become an Expert at Next Gen Penetration Testing and Purple Teaming", 1st Edition, Wiley, 2020.
6. Jon Ericson, Hacking: The Art of Exploitation, 2nd Edition, NoStarch Press, 2008.

List of Experiments:

1. Study of Guessing username and passwords using Hydra. **3**
2. Experiment onRecovering password Hashes
3. Implementation to crack Linux passwords **3**
4. Experiments on SQL injections
5. Analysis of WEP flaws **3**
6. Experiments on Wireless DoS Attacks
7. Implementation of Buffer Overflow Prevention **3**
8. Prevention against Cross Site Scripting Attacking
9. Experiments on Metasploit Framework **3**
10. Implementation to identify web vulnerabilities
11. Wireshark: Experiment to monitor live network capturing packets and analyzing over the live network **3**
12. LOIC: DoS attack using LOIC
13. FTK: Bit level forensic analysis of evidential image and reporting the same. **3**
14. Darkcomet : Develop a malware using Remote Access Tool Darkcomet to take a remote access over network **3**
15. HTTrack: Website mirroring using Httrack and hosting on a local network **3**
16. XSS: Inject a client side script to a web application **3**

17.	Emailtrackerpro: Email analysis involving header check, tracing the route. Also perform a check on a spam mail and non-spam mail	**3**

TOTAL PRACTICAL PERIODS 30 Periods

TOTAL LECTURE CUM PRACTICAL PERIODS 75 Periods

22BM204	**BIOMETRIC DATA PROCESSING**	**L**	**T**	**P**	**C**
		3	**0**	**0**	**3**

Pre-requisite	Nil	**Syllabus Version**	V 0.1

Course Objectives:

1. To understand the basics of Biometric Data processing
2. To model and visualize the transformation of image
3. To understand the evolution of object detection
4. To learn the computational methods involved in the biometric systems

Course Content:

UNIT I INTRODUCTION TO BIOMETRIC DATA PROCESSING 9

Biometric Databases - Biometric traits - Biometric Modalities - Principles of Biometrics: Behavior and Physiology, Data Acquisition, Liveness Detection, Active Biometric Traits-Voice Biometrics, Handwriting Biometrics , Gait Biometrics, Other Active Traits, Passive Biometric Traits- Fingerprint Biometrics, Iris Biometrics, Face Biometrics, ECG Biometrics, Other Passive Traits, Multimodal biometrics -Taxonomy of multimodal biometrics, fusion levels - Biometric Standards.

UNIT II IMAGE PROCESSING FUNDAMENTALS AND OPERATIONS OF BIOMETRIC SYSTEM 10

Image processing and Basic image operations: - pattern recognition/statistics, Error types. image, acquisition, type, point operations, Geometric transformations. Linear interpolation, brightness correction, histogram, Convolution, linear/non-linear filtering, Guassian, Median, Min, gray level reduction. Special filters, enhancement filter, Laplacian, unsharp masking, high boost filtering, sharpening special filtering, Edge detection, DFT , inverse of DFT. Operations of a biometric system - verification and identification, performance of a biometric system, FAR, FRR, GAR, ERR, DET and ROC curve, Failure to Acquire (FTA), Failure to Enroll (FTE), applications of biometrics, characteristics.

UNIT III OBJECT DETECTION AND FACE RECOGNITION 9

Object Detection- Boundary descriptors –Region descriptors –moving object detection – tracking moving features- Moving extraction and description-Texture description – classification - segmentation. Face Recognition – Eigenfaces (PCA), Linear Discriminant Analysis (LDA) and Fisherfaces, Independent Component Analysis (ICA), Neural Networks (NN) and Support Vector Machines (SVM), Kernel Methods, Face biometric database

UNIT IV FINGERPRINT AND IRIS RECOGNITION 9

Fingerprint recognition – Sensing, feature extraction, Enhancement and binarization, Minutiae extraction, matching – correlation based methods, minutiae based methods, ridge feature based methods, performance evaluation, synthetic fingerprint generation IRIS recognition system, Active Contours, Flexible Generalized Embedded Coordinates, Fourierbased Trigonometry and Correction for Off-Axis Gaze, Detecting and excluding eyelashes by Statistical Inference, Alternative Score Normalization Rules

UNIT V 3D BIOMETRIC and BIOMETRIC DATA APPLICATIONS 8

Classification of 3D biometric imaging methods -3D biometric Technologies- 3D palm print capturing systems-3D information in palm print- Feature Extraction from 3D palm print – matching and fusion. Mobile Biometrics- Biometric Application Design – Biometrics in society

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Explain the principles and types of biometric data processing
2. Use Image processing operations for biometrics
3. Apply techniques required for object detection and face recognition
4. Develop techniques required for fingerprint and iris recognition
5. Design and evaluate biometric applications

Text Book(s):

1. Ruud M. Bolle, SharathPankanti, Nalini K. Ratha, Andrew W. Senior, Jonathan H. Connell, “Guide to Biometrics",Springer 2013 (Unit 1)
2. Rafael C. Gonzalez, Richard Eugene Woods, "Digital Image Processing using MATLAB", 2nd Edition, Tata McGraw-Hill Education 2010 (Unit 2)
3. Claus Vielhauer, "Biometric user authentication for IT security: from fundamentals to handwriting", Vol. 18. Springer Science & Business Media, 2005 (Unit 2)
4. Anil Jain, Patrick Flynn, and Arun A. Ross, eds. "Handbook of biometrics", Springer Science & Business Media, 2007 (Unit 3 & 4)
5. Zhang, David, Lu, Guangming, “3D Biometrics Systems and Applications”, Springer 2013. (Unit 5)

Reference Books:

1. Richard O. Duda, David G.Stork, Peter E. Hart, "Pattern Classification", Wiley 2007
2. Julian Ashbourn, "Biometrics in the New World”, Springer 2014.

Web Links:

1. https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/using-biometrics

22BM205	BIOMETRIC DATA PROCESSING LABORATORY	L	T	P	C
		0	0	4	2

Pre-requisite **Syllabus Version** V 0.1

List of Experiments:

1.	Implementation of Image Enhancement	**6**
2.	Implementation of Image Segmentation	**6**
3.	Implementation of Fingerprint Image Acquisition	**6**
4.	Implementation of Fingerprint Feature Extraction	**6**
5.	Implementation of Face Image Acquisition	**6**
6.	Implementation of Face Feature Extraction	**6**
7.	Implementation of Iris Image Acquisition	**6**
8.	Implementation of Iris Feature Extraction	**6**
9.	Implementation of 3D Biometric-Palmprint	**6**
10.	Implementation of Mobile biometrics	**6**
	TOTAL PRACTICAL PERIODS	**60 Periods**

Expected Course Outcome: On completion of the course, the student is expected to

1. Design and Apply Image Enhancement and Segmentation.
2. Design and Apply Fingerprint Acquisition and Feature Extraction
3. Design and Apply Face and Iris Acquisition and Feature Extraction
4. Design and Apply 3D Biometric
5. Implement Mobile Biometrics

Reference Books:

1. Punmia, B.C, “Soil Mechanics and Foundation Engineering”, Laxmi Publishers, New Delhi. 2007.
2. Laboratory Manual, Centre for Water Resources, Anna University, Chennai. 2012.

List of Equipments: (for batch of 30 students)

1.	INTEL based desktop PC with min. 8GB RAM and 500 GB HDD, 17” or higher TFT Monitor, Keyboard and mouse and GPU as required	30 no
2.	Windows 10 or higher operating system / Linux Ubuntu 20 or higher	30 no
3.	OpenBR / OpenFace Tracker/Open EBTS/Insight Face	30 no
4.	Kairos API/Face++/Crypto++ Python 3.9 or higher	30 no

22EEC202	**TERM PAPER WRITING AND SEMINAR**	**L**	**T**	**P**	**C**
		0	**0**	**2**	**1**

Pre-requisite **Syllabus Version** V 0.1

In this course, students will develop their scientific and technical reading and writing skills that they need to understand and construct research articles. A term paper requires a student to obtain information from a variety of sources (i.e., Journals, dictionaries, reference books) and then place itin logically developed ideas. The work involves the following steps:

1. Selecting a subject, narrowing the subject into a topic
2. Stating an objective.
3. Collecting the relevant bibliography (atleast 15 journal papers)
4. Preparing a working outline.
5. Studying the papers and understanding the authors contributions and critically analysingeach paper.
6. Preparing a working outline
7. Linking the papers and preparing a draft of the paper.
8. Preparing conclusions based on the reading of all the papers.
9. Writing the Final Paper and giving final Presentation

Please keep a file where the work carried out by you is maintained.

Activities to be carried out

Activity	**Instructions**	**Submission week**	**Evaluation**
Selection of area of interest and Topic Stating an Objective	You are requested to select an area of interest, topic and state an objective	2nd week	**3 %** Based on clarity of thought, current relevance and clarity in writing
Collecting Information about your area & topic	1. List 1 Special Interest Groups or professional society 2. List 2 journals 3. List 2 conferences, symposia or workshops 4. List 1 thesis title 5. List 3 web presences (mailing lists, forums, news sites) 6. List 3 authors who publish regularly in your area 7. Attach a call for papers (CFP) from your area.	3rd week	**3%** (the selected information must be area specific and of international and national standard)
Collection of Journal papers in the topic in the context of the objective –	1. You have to provide a complete list of references you will be using- Based on your objective -Search various digital libraries and Google Scholar	4th week	**6%** (the list of standardpapers and reason for selection)

collect20 & then filter	2. When picking papers to read - try to: 1. Pick papers that are related to each other in some ways and/or that are in the same field so that you can write a meaningful survey out of them, 2. Favour papers from well-known journals and conferences, 3. Favour “first” or “foundational” papers in the field (as indicated in other people’s survey paper), 4. Favour more recent papers, 5. Pick a recent survey of the field soyou can quickly gain an overview, 6. Find relationships with respect toeach other and to your topic area(classification scheme/categorization) 7. Mark in the hard copy of papers whether complete work or section/sections of the paper are being considered		
Reading and notes for first 5 papers	Reading Paper Process For each paper form a Table answering the following questions: 1. What is the main topic of the article? 2. What was/were the main issue(s) theauthor said they want to discuss? 3. Why did the author claim it wasimportant? 4. How does the work build on other’swork, in the author’s opinion? 5. What simplifying assumptions	5th week	**8%** (the table given should indicate your understanding of the paper and the evaluation is based on your conclusions about each paper)

	doesthe author claim to be making? 6. What did the author do? 7. How did the author claim they weregoing to evaluate their work and compare it to others? 8. What did the author say were thelimitations of their research? 9. What did the author say were theimportant directions for future research? 10. Conclude with limitations/issues not addressed by the paper (from the perspective of your survey)		
Reading and notes for next5 papers	Repeat Reading Paper Process	6th week	**8%** (the table given should indicate your understanding of the paper and the evaluation is based on your conclusions about each paper)
Reading and notes for final 5papers	Repeat Reading Paper Process	7th week	**8%** (the table given should indicate your understanding of the paper and the evaluation is based on your conclusions about each paper)
Draft outline 1 and Linking papers	Prepare a draft Outline, your survey goals,along with a classification / categorization diagram	8th week	**8%** (this component will be evaluated based on the linking and classification among the papers)
Abstract	Prepare a draft abstract and give a presentation	9th week	**6%** (Clarity, purpose and conclusion) **6%** Presentation & Viva Voce
Introduction Background	Write an introduction and background sections	10th week	**5%** (clarity)
Sections of the paper	Write the sections of your paper based on the classification / categorization diagram in keeping with the goals of your survey	11thweek	**10%** (this component will be evaluated based on the linking

			and classification among the papers)
Your conclusions	Write your conclusions and future work	12th week	**5%** (conclusions – clarity and yourideas)
Final Draft	Complete the final draft of your paper	13th week	**10%** (formatting, English, Clarity and linking) **4%** Plagiarism Check Report
Seminar	A brief 15 slides on your paper	14th & 15th week	**10%**(based on presentation and Viva-voce)

TOTAL: 30 PERIODS

22EEC301	PROJECT WORK	L	T	P	C
		0	0	12	6

Pre-requisite **Syllabus Version** V 0.1

Course Objectives:

1. To develop the ability to solve a specific problem right from its identification and literature review till the successful solution of the same.
2. To train the students in preparing project reports and to face reviews and viva voce examination.

The students in a group of 3 to 4 works on a topic approved by the head of the department under the guidance of a faculty member and prepares a comprehensive project report after completing the work to the satisfaction of the supervisor. The progress of the project is evaluated based on a minimum of three reviews. The review committee may be constituted by the Head of the Department. A project report is required at the end of the semester. The project work is evaluated based on oral presentation and the project report jointly by external and internal examiners constituted by the Head of the Department.

TOTAL PRACTICAL PERIODS 300 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. On Completion of the project work students will be in a position to take up any challenging practical problems and find solution by formulating proper methodology.

22EEC401	PROJECT WORK	L	T	P	C
		0	0	24	12

Pre-requisite **Syllabus Version** V 0.1

Course Objectives:

1. To develop the ability to solve a specific problem right from its identification and literature review till the successful solution of the same.
2. To train the students in preparing project reports and to face reviews and viva voce examination.

The students in a group of 3 to 4 works on a topic approved by the head of the department under the guidance of a faculty member and prepares a comprehensive project report after completing the work to the satisfaction of the supervisor. The progress of the project is evaluated based on a minimum of three reviews. The review committee may be constituted by the Head of the Department. A project report is required at the end of the semester. The project work is evaluated based on oral presentation and the project report jointly by external and internal examiners constituted by the Head of the Department.

TOTAL PRACTICAL PERIODS 300 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. On Completion of the project work students will be in a position to take up any challenging practical problems and find solution by formulating proper methodology.

Professional Elective List

22PBM01	PRINCIPLES OF SECURE CODING	L	T	P	C
		3	0	0	3

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. Identify and analyze security problems and their vulnerabilities in software.
2. Understand the various static analysis methods for secure programming.
3.Understand the different secure coding techniques for handling inputs, errors, integer and string operations in a software.
4.Effectively apply their knowledge to write a secure web application

Course Content:

UNIT I SOFTWARE SECURITY 9

Security Concepts, Security Policy, Security Flaws, Vulnerabilities, Exploitation and Mitigations. Software Security problems, Classification of Vulnerabilities.

UNIT II STATIC ANALYSIS 9

Problem Solving with static analysis: Type Checking, Style Checking, Program understanding, verifications and property checking, Bug finding and Security Review.

UNIT III 9

Strings: Common String manipulating Errors, String Vulnerabilities and Exploits, Mitigation Strategies for strings, String handling functions, Runtime protecting strategies, Dynamic Memory. Management: Memory Management errors in C and C++, Notable Vulnerabilities. Integer Security: Integer data Type, Integer Conversions, Integer Operations, Integer Vulnerabilities, Mitigation Strategies.

UNIT IV HANDLING INPUTS AND EXCEPTIONS 9

Handling Inputs: What to validate, How to validate, Preventing metadata Vulnerabilities, Buffer Overflow: Introduction, Exploiting buffer overflow vulnerabilities, Buffer allocation strategies, Tracking buffer sizes, buffer overflow in strings, Buffer overflow in Integers Runtime Protections. Errors and Exceptions: Handling Error with return code, Managing exceptions, Preventing Resource leaks, Logging and debugging

UNIT V SECURE WEB APPLICATIONS 9

Input and Output Validation for the Web: Browser Subverted, HTTP Considerations: Use POST, Not GET, Request Ordering, Error Handling, Request Provenance. Maintaining Session State: Use Strong Session Identifiers, enforce a Session Idle Timeout and a Maximum Session Lifetime, Begin a New Session upon Authentication.

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Apply secure coding practices when developing a software.
2. Understand and perform a static analysis and security review of a software code. 3.
3.Evaluate strings and integer vulnerabilities in a software code.
4. Handle inputs, overflow mechanisms, errors and exceptions in a software code.

5. Design a secure web application by performing input and output validation techniques on the web.

Reference Books:

1. Seacord, R. C., Secure Coding in C and C++, AddisonWesley, Software Engineering Institute, 2nd edition, 2013. (UNIT- III)
2. Chess, B., and West, J., Secure Programming with Static Analysis, Addison Wesley Software Security Series, 2007. (UNIT-II,IV,V)
3. Seacord, R. C., The CERT C Secure Coding Standard, Pearson Education, 2009.
4. Howard, M., LeBlanc, D., Writing Secure Code, 2nd Edition. Pearson Education, 2002.

22PBM02	NETWORK SECURITY	L	T	P	C
		3	0	0	3

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. To learn the fundamentals of cryptography and its application to network security.
2. To understand the mathematics behind cryptography.
3. To learn about the security issues in internet protocol.
4. To understand the security issues in other layers
5. To study about intrusion detection and prevention system and wireless hacking.

Course Content:

UNIT I INTRODUCTION TO NETWORK SECURITY 9

Security Services and Mechanisms – Vulnerabilities in wireless communications –security basics – Attack and its types Security essentials on layers - Electronic signatures – PKI and electronic certificate

UNIT II SYMMETRIC AND ASYMMETRIC CIPHERS 9

Classical Techniques – Substitution Ciphers - Transposition Ciphers. Modern symmetric ciphers: Stream cipher - RC4, Block cipher - DES – AES – Uses of Modes of operation. Modern Asymmetric block ciphers - RSA, ElGamal, MAC – Cryptographic Hash Functions- Key management system- Key Distribution & Key Agreements.

UNIT III SECURITY ISSUES IN INTERNET PROTOCOL 9

Reconnaissance-Wireshark- TCPDump - Netdiscover - Shodan ,NESSUS,Hping3 NSE Scripts: Introduction - How to write and read NSE script - TCP session Hijacking - UDP session Hijacking -HTTP Session – Hijacking - Spoofing basics - IP, DNS and ARP Spoofing

UNIT IV SECURITY IN OTHER LAYERS 9

Email Security and its services – PGP - S/MIME – DNS Security - VPN Concept and its Configuration - AAA Concept, RADIUS, TACACS+ technologies, SSL architecture and protocol.

UNIT V INTRUSION DETECTION AND PREVENTION SYSTEM(IDPS) AND WIRELESS HACKING 9

IDPS introduction - Uses of IDPS Technologies - Key functions of IDPS Technologies, Signature Based Detection, Anomaly Based Detection - Wireless networks - WPA Handshaking – Wireless hacking tools.

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. To design cryptographic algorithms and carry out their implementation.
2. To carry out cryptanalysis on cipher.
3. To be able to design and implement security based internet protocols.
4. To carry out system security for other layers.
5. To understand the importance of intrusion detection and prevention system and wireless hacking. T

Reference Books:

1. Behrouz A. Ferouzan, Debdeep Mukhopadhyay —Cryptography & Network Security, 3rd edition, Tata McGraw Hill, 2015.
2. William Stallings “Network Security Essentials Applications and Standards", Pearson Education., 5th Edition, 2014.
3. Ryan Russell, " Hack Proofing your network ", Wiley,2nd Edition,2002.
4. David M. Durton, “Elementary Number Theory”, Tata Mcgraw Hill, Sixth Edition, 2009.
5. Jonathan Katz, Yehuda Lindell, "Introduction to Modern Cryptography: Principles and Protocols (Chapman & Hall/CRC Cryptography and Network Security Series)", 1st Edition CRC Press Taylor and Francis Group, 2008.
6. Douglas R. Stinson," Cryptography: Theory and Practice, Third Edition (Discrete Mathematics and Its Applications), Chapman & Hall/CRC, 2005.

22PBM03	PUBLIC KEY INFRASTRUCTURE	L	T	P	C
		3	0	0	3

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. Understand public key infrastructure technology
2.Understand Public Key Algorithms
3.Understand centralized and decentralized infrastructure
4.Understand concept of digital certificates
5. Learn various security threats to E-commerce

Course Content:

UNIT I OVERVIEW OF PKI TECHNOLOGY 9

Overview of PKI Technology: Symmetric Vs. Asymmetric Ciphers, PKI Services, PKI Enabled Services, Certificates and Certification, Digital Signatures, Securing Web Transactions, Key and Certificate Life Cycles, PKI Standards, Third Party CA Systems, Secure Socket Layer (SSL), CA System Attacks, Key Escrow Vs Key Recovery, Certification Practices, Securing Business Applications, PKI Readiness.

UNIT II PKI ALGORITHMS 9

Public Key Algorithms, Knapsack, RSA, Pohlig-Hellman, Rabin, Elgamal, McEliece, Elliptic Curve Cryptosystems, LUC, Finite Automation Public Key Cryptosystems, Public Key, Digital Signature Cryptosystems: GOST, ESIGN.

UNIT III DESIGN, IMPLEMENTATION, MANAGEMENT 9

Design, Implementation and Management of PKI: PKI Design Issues, PKI-ROI, Architecture for PKI (APKI), Implementing Secure Web services Requirements using PKI, Versign's Foundation in Managed Security Services, Implementation and Deployment, Implementation Costs, PKI Performance, Obtaining a Certificate, Certification Revocation with Managed PKI, Open Revocation Solutions for Today's Enterprise PKI needs.

UNIT IV E-COMMERCE SECURITY THREATS 9

Security Threats to E-commerce: Internet Security Issues Overview, Intellectual Property Threats, Threats to the Security-Client Computers, Communication Channels, Server Computers, Implementing Electronics Commerce Security: Objects, Protecting- Client Computers, Communication Channels, Web Server, Access Control: Authentication, Authorization and Accountability Controls.

UNIT V 9

Protection in General Purpose Operating Systems: protected objects and methods of protection – memory and address protection – control of access to general objects – file protection Mechanisms – user authentication - Designing Trusted Operating Systems.

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to
1.Compare and contrast various memory management schemes.
2.Design and Implement a prototype file system.

3.Discuss the various synchronization, and memory management issues.

4.Demonstrate the Mutual exclusion, Deadlock detection and agreement protocols of distributed operating system.

5. Discuss the various Security issues.

Reference Books:

1. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, —Operating System Concepts‖, 9th Edition, John Wiley and Sons Inc., 2012.

2. Andrew S. Tanenbaum, —Modern Operating Systems‖, Second Edition, Addison Wesley, 2001.

3. Charles Crowley, —Operating Systems: A Design-Oriented Approach‖, Tata McGraw Hill Education‖, 1996.

4. Charles P. Pleeger, "Security in Computing", Prentice Hall, New Delhi, 2009

5. D M Dhamdhere, —Operating Systems: A Concept-Based Approach‖, Second Edition, Tata 1. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, —Operating System Concepts‖, 9th Edition, John Wiley and Sons Inc., 2012.

2. Andrew S. Tanenbaum, —Modern Operating Systems‖, Second Edition, Addison Wesley, 2001.

3. Charles Crowley, —Operating Systems: A Design-Oriented Approach‖, Tata McGraw Hill Education‖, 1996.

4. Charles P. Pleeger, "Security in Computing", Prentice Hall, New Delhi, 2009

5. D M Dhamdhere, —Operating Systems: A Concept-Based Approach‖, Second Edition, Tata McGraw-Hill Education, 2007.

6. Michael Palmer, Guide to Operating Systems Security‖, Course Technology – Cengage Learning, New Delhi, 2008.

7. William Stallings, —Operating Systems – Internals and Design Principles‖, 7th Edition, Prentice Hall, 2011.

Web Links:

1http://nptel.ac.in/.

22PBM04	OPERATING SYSTEMS SECURITY	L	T	P	C
		3	0	0	3

Pre-requisite	Nil	Syllabus Version	V 0.1

Course Objectives:

1. Understand the structure and functions of OS.

2. Learn about Processes and memory management schemes.

3. Study I/O management and File systems.

4. To gain insight on to the Protection, Security issues

Course Content:

UNIT I FUNDAMENTALS OF OPERATING SYSTEMS 9

Overview – Operating system concepts – Functions – Structure of Operating system – Types of operating system– Dead lock Prevention, Recovery, Detection and Avoidance

UNIT II PROCESS MANAGEMENT 9

Introduction to processes – Process Scheduling - Threads-CPU Scheduling objectives, criteria – Types of scheduling algorithms – Performance comparison – Inter process communications Synchronization – Semaphores.

UNIT III MEMORY MANAGEMENT 9

Single contiguous allocation – Partitioned allocation – Paging – Virtual memory concepts – Swapping – Demand paging – Page replacement algorithms – Segmentation.

UNIT IV DEVICE AND FILE MANAGEMENT 9

Principles of I/O hardware – I/O software – Disks – Disk Scheduling Algorithms--File Systems – Files and Directories- File System Implementation - Allocation Methods.

UNIT V SECURITY ISSUES 9

Protection in General Purpose Operating Systems: protected objects and methods of protection – memory and address protection – control of access to general objects – file protection Mechanisms – user authentication - Designing Trusted Operating Systems.

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1.Compare and contrast various memory management schemes.

2.Design and Implement a prototype file system.

3.Discuss the various synchronization, and memory management issues.

4.Demonstrate the Mutual exclusion, Deadlock detection and agreement protocols of distributed operating system.

5. Discuss the various Security issues.

Reference Books:

1. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, —Operating System Concepts‖, 9th Edition, John Wiley and Sons Inc., 2012.

2. Andrew S. Tanenbaum, —Modern Operating Systems‖, Second Edition, Addison Wesley, 2001.

3. Charles Crowley, —Operating Systems: A Design-Oriented Approach‖, Tata McGraw Hill

Education‖, 1996.

4. Charles P. Pleeger, "Security in Computing", Prentice Hall, New Delhi, 2009

5. D M Dhamdhere, —Operating Systems: A Concept-Based Approach‖, Second Edition, Tata 1. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, —Operating System Concepts‖, 9th Edition, John Wiley and Sons Inc., 2012.

2. Andrew S. Tanenbaum, —Modern Operating Systems‖, Second Edition, Addison Wesley, 2001.

3. Charles Crowley, —Operating Systems: A Design-Oriented Approach‖, Tata McGraw Hill

Education‖, 1996.

4. Charles P. Pleeger, "Security in Computing", Prentice Hall, New Delhi, 2009

5. D M Dhamdhere, —Operating Systems: A Concept-Based Approach‖, Second Edition, Tata McGraw-Hill Education, 2007.

6. Michael Palmer, Guide to Operating Systems Security‖, Course Technology – Cengage Learning, New Delhi, 2008.

7. William Stallings, —Operating Systems – Internals and Design Principles‖, 7th Edition, Prentice Hall, 2011.

Web Links:

1. http://nptel.ac.in/.

22PBM05	SECURITY PRACTICES	L	T	P	C
		3	0	0	3

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. To learn the core fundamentals of system and web security concepts
2. To have through understanding in the security concepts related to networks
3. To deploy the security essentials in IT Sector
4.To be exposed to the concepts of Cyber Security and cloud security
5. To perform a detailed study of Privacy and Storage security and related Issues

Course Content:

UNIT I SYSTEM SECURITY 9

Model of network security – Security attacks, services and mechanisms – OSI security architecture - A Cryptography primer- Intrusion detection system- Intrusion Prevention system - Security web applications- Case study: OWASP - Top 10 Web Application Security Risks.

UNIT II NETWORK SECURITY 9

Internet Security - Intranet security- Local Area Network Security - Wireless Network Security - Wireless Sensor Network Security- Cellular Network Security - Mobile security - IOT security – Case Study - Kali Linux.

UNIT III SECURITY MANAGEMENT 9

Information security essentials for IT Managers- Security Management System - Policy Driven System. Management- IT Security - Online Identity and User Management System. Case study: Metasploit

UNIT IV CYBER SECURITY AND CLOUD SECURITY 9

Cyber Forensics- Disk Forensics – Network Forensics – Wireless Forensics – Database Forensics – Malware Forensics – Mobile Forensics – Email Forensics- Best security practices for automate Cloud infrastructure management – Establishing trust in IaaS, PaaS, and SaaS Cloud types. Case study: DVWA

UNIT V PRIVACY AND STORAGE SECURITY 9

Privacy on the Internet - Privacy Enhancing Technologies - Personal privacy Policies - Detection of Conflicts in security policies- privacy and security in environment monitoring systems. Storage Area Network Security - Storage Area Network Security Devices - Risk management - Physical Security Essentials.

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Understand the core fundamentals of system security
2. Apply the security concepts to wired and wireless networks
3. Implement and Manage the security essentials in IT Sector
4. Explain the concepts of Cyber Security and Cyber forensics
5. Be aware of Privacy and Storage security Issues.

Reference Books:

1. John R. Vacca, Computer and Information Security Handbook, Third Edition, Elsevier 2017
2. Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, Seventh Edition, Cengage Learning, 2022
3. Richard E. Smith, Elementary Information Security, Third Edition, Jones and Bartlett Learning, 2019
4. Mayor, K.K.Mookhey, Jacopo Cervini, Fairuzan Roslan, Kevin Beaver, Metasploit Toolkit for Penetration Testing, Exploit Development and Vulnerability Research, Syngress publications, Elsevier, 2007. ISBN : 978-1-59749-074-0
5. John Sammons, “The Basics of Digital Forensics- The Primer for Getting Started in Digital Forensics”, Syngress, 2012
6. Cory Altheide and Harlan Carvey, “Digital Forensics with Open Source Tools”,2011 Syngress, ISBN: 9781597495875.
7. Siani Pearson, George Yee "Privacy and Security for Cloud Computing" Computer Communications and Networks, Springer, 2013.

22PBM06	MEDIA SECURITY	L	T	P	C
		3	0	0	3

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. To understand the cryptanalysis on standard algorithms meant for confidentiality, integrity and authenticity.
2. To know about Digital rights management.
3. To know about the concepts of Digital Watermarking techniques.
4. To understand the concept of Steganography
5. To learn the privacy preserving techniques on Multimedia data.

Course Content:

UNIT I CRYPTANALYSIS AND DIGITAL RIGHTS MANAGEMENT 9

Cryptanalysis Techniques – Encryption Evaluation metrics – Histogram Deviation – Introduction to DRM – DRM Products –DRM Laws

Suggested Activities: 1. External learning - cryptanalysis for algorithms such as AES, RSA.
2. Analysis for DRM products.

Suggested Evaluation Methods: 1. Group discussion on linear and differential cryptanalysis of cryptographic algorithms. 2. Tutorial on DRM products.

UNIT II DIGITAL WATERMARKING BASICS 9

Introduction – Basics Models of Watermarking – Basic Message Coding – Error Correction coding – Mutual Information and Channel Capacity – Designing a Good Digital Watermark – Information Theoretical Analysis of Digital Watermarking

Suggested Activities: 1. Problems on Error Correction Coding. 2. Designing a good watermark.

Suggested Evaluation Methods: 1. Assignment on ECC. 2. Tutorial on DRM products.

UNIT III DIGITAL WATERMARKING SCHEMES AND PROTOCOLS 9

Spread Spectrum Watermarking – Block DCT-domain Watermarking – Watermarking with Side Information – Dirty-paper Coding – Quantization Watermarking – buyer Seller Watermarking Protocol – Media Specific Digital Watermarking: Image WM, Video WM, Audio WM– Watermarking for CG-Models: Watermarking for Binary Images and 3D Contents – Data Hiding Through Watermarking Techniques.

Suggested Activities: 1. Implementation of buyer seller watermarking protocol.
2. Analyzing the performance of different media specific WM and WM for CG models.

Suggested Evaluation Methods: 1. Tutorial - Media specific watermarking techniques.
2. Group discussion on the performance evaluation of watermarking techniques.

UNIT IV STEGANOGRAPHY AND STEGANALYSIS 9

Stenographic Communication – Notation and Terminology – Information –Theoretic Foundations of Steganography – Cachin's Definition of Steganographic Security – Statistics Preserving Steganography – Model-Based Steganography – Masking Embedding as Natural Processing – Minimizing the Embedding Impact – Matrix Embedding –Nonshared Selection Rule – Steganalysis Algorithms: LSB Embedding and the Histogram Attack – Sample Pairs Analysis.

Suggested Activities:

1. An application to be developed using Steganography.

Suggested Evaluation Methods:

1. Can be done by hiding capacity, Distortion measure and Security
2. Project.

UNIT V MULTIMEDIA ENCRYPTION 9

Multimedia Processing in the Encryption Domain – Information Processing – Data Sanitization – Finger Printing – Digital Forensics: Intrusive and Non- Intrusive – Forgeries Detection– Privacy Preserving – Surveillance.

Suggested Activities:
1. Case study on forensic data.
2. Case study on forgery detection.

Suggested Evaluation Methods:
1. Group discussion on case studies

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to
1. Identify the security challenges and issues that may arise in any system.
2. Implement the concepts of steganography, digital watermarking techniques.
3. Design secure applications using steganography and watermarking schemes
4. Apply concepts on digital rights management while developing secure systems
5. Design a secure multimedia system using encryption and privacy preservation techniques.

Reference Books:

1. Frank Shih, “Digital Watermarking and Steganography: Fundamentals and Techniques”, CRC Press,Second Edition 2017.
2. Fathi E. Abd El-Samie, HossamEldin H. Ahmed, Ibrahim F. Elashry, Mai H. Shahieen, Osama S. Faragallah, El-Sayed M. El-Rabaie, Saleh A. Alshebeili , “Image Encryption: A Communication Perspective”, CRC Press,First Edition 2013.
3. Douglas R. Stinson, “Cryptography Theory and Practice”, Fourth Edition, Chapman & Hall/CRC, 2006 .
4. Wenbo Mao, “Modern Cryptography – Theory and Practice”, Pearson Education, 2006.
5. Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich and TonKalker, “Digital Watermarking and Steganography”, Second Edition, Elsevier, 2007.

22PBM07	BIOMETRIC SECURITY	L	T	P	C
		3	0	0	3

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. To understand the technologies of fingerprint, iris, face and speech recognition
2. To understand the general principles of design of biometric systems and the underlying trade-offs.
3. To recognize personal privacy and security implications of biometrics based identification technology.
4. To identify issues in the realistic evaluation of biometrics based systems.

Course Content:

UNIT I INTRODUCTION TO BIOMETRICS 9

Introduction and back ground – biometric technologies – passive biometrics – active biometrics - Biometrics Vs traditional techniques – Benefits of biometrics - Operation of a biometric system– Key biometric processes: verification, identification and biometric matching – Performance measures in biometric systems: FAR, FRR, FTE rate, FTA rate and rate- Need for strong authentication – Protecting privacy and biometrics and policy – Biometric applications

UNIT II FINGERPRINT IDENTIFICATION TECHNOLOGY 9

Fingerprint Patterns, Fingerprint Features, Fingerprint Image, and width between two ridges - Fingerprint Image Processing - Minutiae Determination - Fingerprint Matching: Fingerprint Classification, Matching policies.

UNIT III FACE RECOGNITION 9

Introduction, components, Facial Scan Technologies, Face Detection, Face Recognition, Representation and Classification, Kernel- based Methods and 3D Models, Learning the Face Spare, Facial Scan Strengths and Weaknesses, Methods for assessing progress in Face Recognition

UNIT IV VOICE SCAN 9

Introduction, Components, Features and Models, Addition Method for managing Variability, Measuring Performance, Alternative Approaches, Voice Scan Strengths and Weaknesses, NIST Speaker Recognition Evaluation Program, Biometric System Integration.

UNIT V FUSION IN BIOMETRICS 9

Introduction to Multibiometric - Information Fusion in Biometrics - Issues in Designing a Multibiometric System - Sources of Multiple Evidence - Levels of Fusion in Biometrics - Sensor level, Feature level, Rank level, Decision level fusion - Score level Fusion. Examples – biopotential and gait based biometric systems.

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Demonstrate knowledge engineering principles underlying biometric systems.
2. Analyses design basic biometric system applications.

Text Book(s):

1.James Wayman, Anil Jain, Davide Maltoni, Dario Maio, “Biometric Systems, Technology Design and Performance Evaluation”, Springer, 2005.

2. David D. Zhang, “Automated Biometrics: Technologies and Systems”, Kluwer Academic Publishers, New Delhi, 2000.

3. Arun A. Ross , Karthik Nandakumar, A.K.Jain, “Handbook of Multibiometrics”, Springer, New Delhi, 2006.

Reference Books:

1.Paul Reid, “Biometrics for Network Security”, Pearson Education, 2004.

2. Nalini K Ratha, Ruud Bolle, “Automatic fingerprint Recognition System”, Springer, 2003

3. L C Jain, I Hayashi, S B Lee, U Halici, “Intelligent Biometric Techniques in Fingerprint and Face Recognition” CRC Press, 1999.

4. John Chirillo, Scott Blaul, “Implementing Biometric Security”, John Wiley, 2003.

5. S.Y. Kung, S.H. Lin, M.W.Mak, “Biometric Authentication: A Machine Learning Approach”Prentice Hall, 2005

22PBM08	SECURE SYSTEMS ENGINEERING	L	T	P	C
		3	0	0	3

Pre-requisite	Nil	**Syllabus Version**	V 0.1

Course Objectives:

1. Study of designing secure systems.
2. Understand the micro architectural level of security.
3. Understand hardware, operating system, and application layer vulnerabilities.
4. Study countermeasures for system level attacks.

Course Content:

UNIT I HARDWARE SECURITY 9

Hardware Security - Hardware Trojans and Detection, PUFs - Power Analysis Attacks and Countermeasures - Fault Attacks - Implementation Aspects of Crypto Algorithms (A case study of AES and ECC)

UNIT II MICRO ARCHITECTURAL SECURITY 9

Micro Architectural Security - Timing attacks and Covert Channels - RAM based attacks - Cold boot – Row hammer

UNIT III OPERATING SYSTEM SECURITY 9

Operating System Security - Stack Smashing Attacks - Dynamic Memory Allocation Attacks – Format String Vulnerabilities - return-to-libc attacks - ROP attacks - Side Channel Attacks in Operating Systems - Countermeasures - Non-executable stacks - Capability based Systems - Canaries -Malware Analysis Techniques

UNIT IV APPLICATION SECURITY 9

Application Security SQL Insertion - ShellShock - Heart bleed bug, Covert Channels, Flush+Reload Attacks, Prime+Probe, Meltdown, Spectre

UNIT V SYSTEMS SECURITY 9

Systems Security- Formal Verification of Security Protocols, Power Analysis Attacks, PowerAnalysisAttacks, Hardware Trojans, FANCI: Identification of Stealthy Malicious Logic, Detecting Hardware Trojans in ICs, Protecting against Hardware Trojans, Side Channel Analysis, Fault Attacks on AES

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Identify and analyse vulnerabilities at hardware level
2. Identify micro architectural level security
3. Analyse and apply countermeasures to operating system level attacks
4. Apply malware analysis techniques at system level
5. Understand and analyse application level security

Reference Books:

1. Chester Rebeiro, Debdeep Mukhopadhyay and Sarani Bhattacharya, "Timing Channels in Cryptography, A Micro- Architectural Perspective ", Springer, 2015
2. Secure Systems Engineering, https://nptel.ac.in/courses/106/106/106106199 (Unit 4,5)
3. Swarup Bhunia, Mark Tehranipoor, “Hardware Security: A Hands-on Learning Approach”, Morgan Kauffmann, 2018.
4. S. Garfinkel and L. F. Cranor, "Security and Usability: Designing Secure Systems That People Can Use", O’Reilly, 2008
5. Matt Bishop , "Computer Security: Art and Science”, 2nd Edition, Addison-Wesley, 2018.

22PBM09	**CLOUD SECURITY**	**L**	**T**	**P**	**C**
		3	**0**	**0**	**3**

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1.To Introduce Cloud Computing terminology, definition & concepts

2.To understand the security design and architectural considerations for Cloud

3.To understand the Identity, Access control in Cloud

4.To follow best practices for Cloud security using various design patterns

5.To be able to monitor and audit cloud applications for security

Course Content:

UNIT I FUNDAMENTALS OF CLOUD COMPUTING 9

Understand what is Cloud computing, Architectural and Technological Influences of Cloud Computing, Understand the 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 9

Guiding Security design principles for Cloud Computing, Comprehensive data protection, End-to end access control, CSA, NIST and ENISA guidelines for Cloud Security, Common attack vectors and threats, Compute, Network and Storage, Secure Isolation Strategies, Multitenancy, Virtualization strategies, Inter-tenant network segmentation strategies, Storage isolation strategies, Data Protection strategies, Data retention, deletion and archiving procedures for tenant data, Encryption, Data Redaction, Tokenization, Obfuscation, PKI and Key

UNIT III ACCESS CONTROL AND IDENTITY MANAGEMENT 9

Understand the access control requirements for Cloud infrastructure, Enforcing Access Control Strategies, Authentication and Authorization, Roles-based Access Control, Multi-factor authentication, Host, storage and network access control options, OS Hardening and minimization, securing remote access, Verified and measured boot, Firewalls, Intruder Detection, Intruder prevention and honeypots, User Identification, authentication, and Authorization in Cloud Infrastructure, Identity & Access Management, Single Sign-on, Identity Federation, Identity providers and service consumers, The role of Identity provisioning

UNIT IV CLOUD SECURITY DESIGN PATTERNS 9

Introduction to Design Patterns, Platform-to-Virtualization & Virtualization-to-Cloud, Cloud bursting, Geo-tagging, Cloud VM Platform Encryption, Secure Cloud Interfaces, Cloud Resource Access Control, Secure On-Premise Internet Access, Secure External Cloud Connection, Cloud Denial-of-Service Protection, Cloud Traffic Hijacking Protection, Cloud Authentication Gateway, Federated Cloud Authentication, Cloud Key Management

UNIT V MONITORING, AUDITING AND MANAGEMENT 9

Proactive activity monitoring, Incident Response, Monitoring for unauthorized access, malicious traffic, abuse of system privileges, 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

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Understand the cloud concepts and fundamentals.
2. Explain the security challenges in cloud.
3. Define cloud policy and Identity and Access Managements.
4. Understand various risks, and audit and monitoring mechanisms in cloud.
5. Define the various architectural and design considerations for security in cloud

Reference Books:

1. Raj Kumar Buyya , James Broberg, andrzej Goscinski, ―Cloud Computing:‖, Wiley 2013
2. Dave shackleford, ―Virtualization Security‖, SYBEX a wiley Brand 2013.
3. Mather, Kumaraswamy and Latif, ―Cloud Security and Privacy‖, OREILLY 2011
4. Mark C. Chu-Carroll ―Code in the Cloud‖,CRC Press, 2011
5. Mastering Cloud Computing Foundations and Applications Programming Rajkumar Buyya, Christian Vechhiola, S. Thamarai Selvi

22PBM10	FIREWALL AND VPN SECURITY	L	T	P	C
		3	0	0	3

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1.Identify and assess current and anticipated security risks and vulnerabilities
2.Develop a network security plan and policies
3. Establish a VPN to allow IPsec remote access traffic
4.Monitor, evaluate and test security conditions and environment
5. Develop critical situation contingency plans and disaster recovery plan
6.Implement/test contingency and backup plans and coordinate with stakeholders
7.Monitor, report and resolve security problems

Course Content:

UNIT I INTRODUCTION 9

Introduction, Types of Firewalls, Ingress and Egress Filtering, Types of Filtering, Network Address Translation (NAT), Application Proxy, Circuit Proxy, Content Filtering, Software versus Hardware.Firewalls, IPv4 versus IPv6 Firewalls, Dual-Homed and Triple-Homed Firewalls, Placement of Firewalls.

UNIT II VPN FUNDAMENTALS 9

VPN Deployment Models and Architecture, Edge Router, Corporate Firewall, VPN Appliance, Remote Access, Site-to-Site, Host-to-Host, Extranet Access, Tunnel versus Transport Mode, The Relationship Between Encryption and VPNs, Establishing VPN Connections with Cryptography, Digital Certificates, VPN Authorization.

UNIT III EXPLORING THE DEPTHS OF FIREWALLS 9

Firewall Rules, Authentication and Authorization, Monitoring and Logging, Understanding and Interpreting Firewall Logs and Alerts, Intrusion Detection, Limitations of Firewalls, Downside of Encryption with Firewalls, Firewall Enhancements, and Management Interfaces.

UNIT IV OVERVIEW OF INDUSTRIAL CONTROL SYSTEMS 9

Overview of SCADA, DCS, and PLCs, ICS Operation, Key ICS Components, Control Components, Network Components, SCADA Systems, Distributed Control Systems, Programmable Logic Controllers, Industrial Sectors and Their Interdependencies.

UNIT V SCADA PROTOCOLS 9

Modbus RTU, Modbus TCP/IP, DNP3, DNP3 TCP/IP, OPC, DA/HAD, SCADA protocol fuzzing, Finding Vulnerabilities in HMI: software- Buffer Overflows, Shell code. Previous attacks Analysis Stuxnet, Duqu.

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to
CO1: Show the fundamental knowledge of Firewalls and it types

CO2: Construct a VPN to allow Remote Access, Hashing, connections with Cryptography and VPN Authorization
CO3: Elaborate the knowledge of depths of Firewalls, Interpreting firewall logs, alerts, Intrusion and Detection
CO4: Explain the design of Control Systems of SCAD, DCS, PLC‘s and ICS‘s
CO5: Evaluate the SCADA protocols like RTU, TCP/IP, DNP3, OPC,DA/HAD

Reference Books:

J. Michael Stewart and Denise Kinsey "Network Security, Firewalls, and VPNs", 3rd Edition, Jones & Bartlett Learning, October 2020, ISBN: 9781284183696
2. T. Macaulay and B. L. Singer, Cyber security for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS, Auerbach Publications, 2011.
3. J. Lopez, R. Setola, and S. Wolthusen, Critical Infrastructure Protection Information Infrastructure Models, Analysis, and Defense, Springer-Verlag Berlin Heidelberg, 2012.
4. Robert Radvanovsky and Jacob Brodsky, editors. Handbook of SCADA/Control Systems Security. Routledge, 2020, ISBN 9780367596668.
5. A.W. Colombo, T. Bangemann, S. Karnouskos, S. Delsing, P. Stluka, R. Harrison, et al. Industrial cloud-based cyber-physical systems Springer International Publishing, 2014
6. D. Bailey, Practical SCADA for Industry. Burlington, MA: Newnes, 2003.

22PBM11	DIGITAL AND MOBILE FORENSICS	L	T	P	C
		3	0	0	3

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1.To understand basic digital forensics and techniques.
2.To understand digital crime and investigation.
3. To understand how to be prepared for digital forensic readiness.
4. To understand and use forensics tools for iOS devices.
5.To understand and use forensics tools for Android devices.

Course Content:

UNIT I DIGITAL AND MOBILE FORENSICS 6

Forensic Science – Digital Forensics – Digital Evidence – The Digital Forensics Process – Introduction – The Identification Phase – The Collection Phase – The Examination Phase – The Analysis Phase – The Presentation Phase

UNIT II DIGITAL CRIME AND INVESTIGATION 6

Digital Crime – Substantive Criminal Law – General Conditions – Offenses – Investigation Methods for Collecting Digital Evidence – International Cooperation to Collect Digital Evidence

UNIT III DIGITAL FORENSIC READINESS 6

Introduction – Law Enforcement versus Enterprise Digital Forensic Readiness – Rationale for Digital Forensic Readiness – Frameworks, Standards and Methodologies – Enterprise Digital Forensic Readiness – Challenges in Digital Forensics

UNIT IV iOS FORENSICS 6

Mobile Hardware and Operating Systems - iOS Fundamentals – Jailbreaking – File System – Hardware – iPhone Security – iOS Forensics – Procedures and Processes – Tools – Oxygen Forensics – MobilEdit – iCloud

UNIT V ANDROID FORENSICS 6

Android basics – Key Codes – ADB – Rooting Android – Boot Process – File Systems – Security – Tools – Android Forensics – Forensic Procedures – ADB – Android Only Tools – Dual Use Tools – Oxygen Forensics – MobilEdit – Android App Decompiling

TOTAL LECTURE PERIODS 30 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Have knowledge on digital forensics.
2. Know about digital crime and investigations.
3. Be forensic ready.
4. Investigate, identify and extract digital evidence from iOS devices.
5. Investigate, identify and extract digital evidence from Android devices.

Text Book(s):

1. Andre Arnes, “Digital Forensics”, Wiley, 2018.
2. Chuck Easttom, “An In-depth Guide to Mobile Device Forensics”, First Edition, CRC Press, 2022.

Reference Books:

Vacca, J, Computer Forensics, Computer Crime Scene Investigation, 2nd Ed, Charles River Media, 2005, ISBN: 1-58450-389.

22PBM12	**Access Control and Identity Management Systems**	**L**	**T**	**P**	**C**
		3	**0**	**0**	**3**

Pre-requisite	Nil	**Syllabus Version**	V 0.1

Course Objectives:

1.To understand the importance of Identity Access and Management (IAM),

2.To understand the regulations and industry standards for Identity management

3.To build the capability to assess the risks, understand the techniques for Identity and authentication

4.To learn and devise various access control techniques and access control systems

5.To do typical case studies of online applications

Course Content:

UNIT I INTRODUCTION 9

Why IAM – roadmap to IAM- concepts of identity and access-The Need for Identity Management Who Is in the IT Environment-The Need to Provide Access to Multiple Resources. COMPLYING WITH REGULATIONS - Health Insurance Portability and Accountability Act (HIPAA), Federal Security Information Security Act (FISMA)Sarbanes-Oxley Act. Managing Identities in Distributed Environments Effective identity management. INDUSTRY STANDARDS FOR IDENTITY MANAGEMENT- Industry standard protocols to enable cost-effective identity management - Service Provisioning Markup Language (SPML), Security Assertions Markup Language (SAML), extensible Access Control Markup Language (XACML), Lightweight Directory Access Protocol (LDAP) and X.500, Directory Services Markup Language (DSML), Universal Description Discovery Integration (UDDI), Web Services Security (WS-S).

UNIT II IDENTITY MANAGEMENT 9

Business Drivers, Identity and Access Management- key Concepts, Adoption risks, components, Administration of Access Rights and Entitlements, provisioning process and enforcement process, use of technology in IAM, auditing IAM. Managing identity including Internet of Things. Identification and Authentication Techniques -Passwords, Biometrics, Tokens, Tickets, Single Sign-on (SSO), Multiple Authentication Factors.

UNIT III ACCESS MANAGEMENT 9

Types of access control, Layered access controls and “defense in depth”, The Process of Accountability. Access Control Techniques- Discretionary Access Controls (DAC), Non Discretionary Access Controls (NAC), Mandatory Access Controls (MAC), Role-Based Access Controls (RBAC), Task Based Access Controls (TBAC), Lattice-Based Access Controls. Access Control Methodologies and Implementations - Access Control Administration – Account Administration - Account, Log, and Journal Monitoring/Audits- Access Rights and Permissions

UNIT IV ACCESS CONTROL SYSTEMS 9

Security, Identity Management and Trust Models Current access management technologies. Authentication technologies-overview, authentication by third parties, choosing an authentication system. Authorization based on physical location-IP address-based licensing, Authorization based on user identity or affiliation.

UNIT V CASE STUDIES 9

Technology, Architecture and Controlling Access to Online/Mobile Applications-Library, Banking and Shopping

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Understand the role of IAM with emerging mobile information society, compliance and regulations and industry standards for Identity management.
2. Perform risks assessment
3. Compare various access control techniques.
4. Choose the appropriate Programming Models and approach
5. Carry out analysis and report strength and weakness if IAM in a given typical online Applications.

Reference Books:

1. MessaoudBenantar, ”Access Control Systems: Security, Identity Management and Trust Models”, IBM Corp, Austin, TX, USA. Library of Congress, ISBN-13: 978-0-387-00445-7 e-ISBN-13: 978-0-387-27716-5.

2. Masha Garibyan, Simon McLeish and John Paschoud, “Access and Identity Management for Libraries: Controlling access to online information”, Facet Publishing 2014 www.facetpublishing.co.uk.

3. Frank Bresz, Ernst & Young LLP et. al., “Identity and Access Management GTAG'', The Institute of Internal Auditors, Altamonte Springs, FL32701-4201. 2007.

4. Ray Wagner, “Identity and Access Management”, Digital 2020, ISSA Journal, June 2014 , www.issa.org.

5. Dan Sullivan, “The Definitive Guide to Security Management”, Realtimepublishers.com chapter5: Identity and Access Management http://www3.ca.com/ebook/.

6. Elena Ferrari and M. Tamer A-zsu, “Access Control in Data Management Systems”, Morgan & Claypool Publishers, 2010

22PBM13	SOCIAL NETWORK ANALYSIS	L	T	P	C
		3	0	0	3

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. Formalise different types of entities and relationships as nodes and edges and represent this information as relational data.
2. Understand the fundamental concepts in analyzing the large-scale data that are derived from social networks
3. Understand the basic concepts and principles of different theoretical models of social networks analysis
4. Transform data for analysis using graph-based and statistics-based social network measures
5. Choose among social network designs based on research goals

Course Content:

UNIT I GRAPH THEORY AND STRUCTURE 9

Breadth First Search (BFS) Algorithm. Strongly Connected Components (SCC) Algorithm. Weakly Connected Components (WCC) Algorithm. First Set of Experiments—Degree Distributions. Second Set of Experiments—Connected Components. Third Set of Experiments—Number of Breadth First Searches. Rank Exponent R. Out-Degree Exponent O. Hop Plot Exponent H. Eigen Exponent E. Permutation Model. Random Graphs with Prescribed Degree Sequences. Switching Algorithms. Matching Algorithm. "Go with the Winners" Algorithm. HyperANF Algorithm. Iterative Fringe Upper Bound (iFUB) Algorithm. Spid. Degree Distribution. Path Length. Component Size. Clustering Coefficient and Degeneracy. Friends-of-Friends. Degree Assortativity. Login Correlation.

UNIT II SOCIAL NETWORK GRAPH ANALYSIS 9

Social network exploration/ processing and properties: Finding overlapping communities, similarity between graph nodes, counting triangles in graphs, neighborhood properties of graphs. Pregel paradigm and Apache Giraph graph processing system.

UNIT III INFORMATION DIFFUSION IN SOCIAL NETWORKS 9

Strategic network formation: game theoretic models for network creation/ user behavior in social networks. Information diffusion in graphs: Cascading behavior, spreading, epidemics, heterogeneous social network mining, influence maximization, outbreak detection. Opinion analysis on social networks: Contagion, opinion formation, coordination and cooperation.

UNIT IV CASCADING IN SOCIAL NETWORKS 8

Cascading in Social Networks. Decision Based Models of Cascade. Collective Action. Cascade Capacity. Co-existence of Behaviours. Cascade Capacity with Bilinguality. Probabilistic Models of Cascade. Branching Process. Basic Reproductive Number. SIR Epidemic Model. SIS Epidemic Model. SIRS Epidemic Model. Transient Contact Network. Cascading in Twitter.

UNIT V LINK ANALYSIS & COMMUNITY DETECTION 9

Search Engine. Crawling. Storage. Indexing. Ranking. Google. Data Structures. Crawling. Searching. Web Spam Pages Strength of Weak Ties. Triadic Closure. Detecting Communities in a Network. Girvan-Newman Algorithm. Modularity. Minimum Cut Trees. Tie Strengths in Mobile Communication Network. Exact Betweenness Centrality. Approximate Betweenness Centrality.

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Plan and execute network analytical computations.
2. Implement mining algorithms for social networks
3. Analyze and evaluate social communities.
4. Use social network analysis in behavior analytics
5. Perform mining on large social networks and illustrate the results.

SUGGESTED ACTIVITIES:

1. Twitter Intelligence project performs tracking and analysis of the Twitter
2. Large-Scale Network Embedding as Sparse Matrix Factorization
3. Implement how Information Propagation on Twitter
4. Social Network Analysis and Visualization software application.
5. Implement the Structure of Links in Networks

Text Book(s):

1. Social Network Analysis: Methods & Applications, Stanley Wasserman, And Katherine F' Aust. Cambridge University Press, 2012
2. Practical Social Network Analysis with Python, Krishna Raj P. M. Ankith Mohan and K. G. Srinivasa. Springer, 2018

Reference Books:

1. Social Network Analysis: History, Theory and Methodology by Christina Prell, SAGE Publications, 1st edition, 2011
2. Sentiment Analysis in Social Networks, Federico Alberto Pozzi, Elisabetta Fersini, Enza Messina, and Bing. LiuElsevier Inc, 1st edition, 2016

22PBM14	DATA PRIVACY	L	T	P	C
		3	0	0	3

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1.To understand the basics of data privacy

2.To create architectural, algorithmic and technological foundations for the maintenance of the privacy

3. To become knowledgeable in Static Data Anonymization Methods.

4. To analyse anonymization algorithms

5. To understand the concept of privacy preservation

Course Content:

UNIT I INTRODUCTION 9

Data Privacy and its importance, Need for Sharing Data, Methods of Protecting Data, Importance of Balancing Data Privacy and Utility, Disclosure, Tabular Data, Micro data, Approaches to Statistical disclosure control, Ethics, principles, guidelines and regulations, Microdata concepts, Disclosure, Disclosure risk, Estimating re-identification risk, Non-perturbative microdata masking, Perturbative microdata masking, Information loss in microdata

UNIT II STATIC DATA ANONYMIZATION ON MULTIDIMENSIONAL DATA 9

Static Data Anonymization on Multidimensional Data, Classification of Privacy Preserving Methods, Classification of Data in a Multidimensional Data Set, Group-Based Anonymization, k-Anonymity, lDiversity, t-closeness

UNIT III STATIC DATA ANONYMIZATION ON COMPLEX DATA STRUCTURES 9

Static Data Anonymization on Complex Data Structures, Privacy Preserving Graph Data, Privacy Preserving Time Series Data, Time Series Data Protection Methods, Privacy Preservation of Longitudinal Data, Privacy Preservation of Transaction Data

UNIT IV STATIC DATA ANONYMIZATION ON THREATS TO ANONYMIZED DATA 9

Static Data Anonymization on Threats to Anonymized Data, Threats to Data Structures, Threats by Anonymization Techniques, Randomization, k-Anonymization, l-Diversity, t-Closeness. Dynamic Data Protection: Tokenization, Understanding Tokenization, Use Cases for Dynamic Data Protection, Benefits of Tokenization Compared to Other Methods, Components for Tokenization.

UNIT V PRIVACY PRESERVING 9

Privacy Preserving, Data Mining: Key Functional Areas of Multidimensional Data, Association Rule Mining, Clustering - Privacy Preserving Test Data Manufacturing Generation, Test Data Fundamentals, Utility of Test Data: Test Coverage, Privacy Preservation of Test Data, Quality of Test Data, Anonymization Design for PPTDG, Insufficiencies of Anonymized Test.

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Become familiar with the basics of privacy.
2. Understand how privacy is formalized.
3. Understand the common data privacy techniques.
4. Able to analyse Static Data Anonymization
5. Understand and analyse privacy preservation techniques

Reference Books:

1. N. Venkataramanan and A. Shriram, "Data privacy: Principles and practice". CRC Press, 2016. ISBN: 978-1-49-872104-2

2. A. Hundepool, J. Domingo-Ferrer, L. Franconi, S. Giessing, and E. S. Nordholt, P.D. Wolf, “Statistical disclosure control”, Wiley, John & Sons, 2012. ISBN No.: 978-1-11-997815-2

3. G. T. Duncan, M. Elliot, J.-J. Salazar-González, J.-J. Salazar-Gonzalez, and J. J. Salazar, "Statistical confidentiality: Principles and practice", Springer-Verlag New York, 2011. ISBN: 978-1-44-197801-1

4. C. C. Aggarwal and P. S. Yu, "Privacy-preserving data mining: Models and Algorithms", Springer-Verlag New York, 2008. (ISBN No.: 978-0-387-70992-5)

22PBM15	**SECURITY IN CYBER-PHYSICAL SYSTEMS**	**L**	**T**	**P**	**C**
		3	**0**	**0**	**3**

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. To learn about design of cyber-physical systems
2. To know about MATLAB usage
3. To learn about analysis of cyber-physical systems
4. How to implement safety assurance in these systems
5. To do the software analysis
6. To know basic security measures to take in Cyber-Physical Systems

Course Content:

UNIT I INTRODUCTION TO CYBER-PHYSICAL SYSTEMS 6

Cyber-Physical Systems (CPS) in the real world, Basic principles of design and validation of CPS, Industry 4.0, AutoSAR, IIOT implications, Building Automation, Medical CPS.

UNIT II CPS - PLATFORM COMPONENTS 10

CPS - Platform components: CPS HW platforms - Processors, Sensors, Actuators, CPS Network - WirelessHart, CAN, Automotive Ethernet, CPS Sw stack – RTOS, Scheduling Real Time control tasks Principles of Automated Control Design: Dynamical Systems and Stability Controller Design Techniques, Stability Analysis: CLFs, MLFs, stability under slow switching, Performance under Packet drop and Noise

UNIT III USING MATLAB 8

Matlab toolboxes - Simulink, Stateflow CPS implementation: From features to software components, Mapping software components to ECUs, CPS Performance Analysis - effect of scheduling, bus latency, sense and actuation faults on control performance, network congestion

UNIT IV CPS SAFETY ASSURANCE AND SOFTWARE ANALYSIS 12

Formal Methods for Safety Assurance of Cyber-Physical Systems: Advanced Automata based modeling and analysis, Basic introduction, and examples, Timed and Hybrid Automata, Definition of trajectories, Formal Analysis: Flow pipe construction, reachability analysis Analysis of CPS Software: Weakest Pre-conditions, Bounded Model checking, CPS SW Verification: Frama-C, CBMC Secure Deployment of CPS: Attack models, Secure Task mapping and Partitioning, State estimation for attack detection Automotive Case study: Vehicle ABS hacking Power Distribution Case study: Attacks on Smart Grids

UNIT V CPS SECURITY 9

CPS vulnerabilities, threats, attacks & failures, CPS security threats, CPS vulnerabilities, Cyber- physical system attacks, CPS failures, Evaluating risks, Securing CPS, CPS security challenges, CPS security solutions, CPS forensics, Limitations, CPS protection recommendations

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Understand the core principles behind CPS.
2. Identify safety specifications and critical properties.
3. Understand abstraction in system designs.
4. Express pre and postconditions and invariants for CPS models.
5. Identify CPS security threats and do the software analysis.

Text Book(s):

1. Raj Rajkumar, Dionisio De Niz , and Mark Klein, Cyber-Physical Systems, Addison-Wesley Professional
2. Rajeev Alur, Principles of Cyber-Physical Systems, MIT Press, 2015.
3. André Platzer, Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics., Springer, 2010. 426 pages,ISBN 978-3-642-14508-7.

Reference Books:

1. Jean J. Labrosse, Embedded Systems Building Blocks: Complete and Ready-To-Use
2. Jean-Paul A. Yaacoub, Ola Salman, Hassan N. Noura, NesrineKaaniche, Ali Chehab, Mohamad Malli, "Cyber-physical systems security: Limitations, issues and future trends", Microprocessors and Microsystems, Vol 77, 2020, ISSN 0141-9331 (Unit 5)
3. Sajal Das, Krishna Kant, and Nan Zhang, "Handbook on Securing Cyber-Physical CriticalInfrastructure – Foundations & Challenges", Morgan Kaufmann, 2012

22PBM16	CRYPTANALYSIS	L	T	P	C
		3	0	0	3

Pre-requisite	Nil	**Syllabus Version**	V 0.1

Course Objectives:

1. To understand the importance of cryptanalysis in our increasingly computer-driven world.
2. To understand the fundamentals of Cryptography
3. To understand the Lattice- based cryptanalysis and elliptic curves and pairings
4. To understand birthday- based algorithms for functions and attacks on stream ciphers
5. To apply the techniques for secure transactions in real world applications

Course Content:

UNIT I INTRODUCTION 9

Preliminaries, Defining Security in Cryptography, Monoalphabetic Ciphers: Using Direct Standard Alphabets, The Caesar Cipher, Modular arithmetic, Direct Standard alphabets, Solution of direct standard alphabets by completing the plain component, Solving direct standard alphabets by frequency considerations, Alphabets based on decimations of the normal sequence, Solution of decimated standard alphabets, Monoalphabets based on linear transformation. Polyalphabetic Substitution: Polyalphabetic ciphers, Recognition of polyalphabetic ciphers, Determination of number of alphabets, Solution of individual alphabets if standard, Polyalphabetic ciphers with a mixed plain sequence, Matching alphabets, Reduction of a polyalphabetic cipher to a monoalphabetic ciphers with mixed cipher sequences

UNIT II TRANSPOSITION 9

Columnar transposition, Solution of transpositions with Completely filled rectangles, incompletely filled rectangles, Solution of incompletely filled rectangles – Probable word method, Incompletely filled rectangles general case, Repetitions between messages; identical length messages. Sieve algorithms: Introductory example: Eratosthenes's sieve, Sieving for smooth composites

UNIT III BRUTE FORCE CRYPTANALYSIS 9

Introductory example: Dictionary attacks, Brute force and the DES, Algorithm, Brute force as a security mechanism, Brute force steps in advanced cryptanalysis, Brute force and parallel computers. The birthday paradox: Sorting or not?: Introductory example: Birthday attacks on modes of operation, Analysis of birthday paradox bounds, Finding collisions, Application to discrete logarithms in generic groups.

UNIT IV ALGORITHMS FOR FUNCTIONS 9

Birthday- based algorithms for functions: algorithmic aspects, analysis of random functions, number-theoretic applications, a direct cryptographic application in the context of blockwide security, collisions in hash functions. attacks on stream ciphers: LFSR-based key stream generators, correlation attacks, noisy LFSR model, algebraic attacks, extension to some non- linear shift registers, the cube attack.

UNIT V LATTICE BASED CRYPTANALYSIS 9

Direct attacks using lattice reduction, Coppersmith’s small roots attacks. Elliptic curves and pairings: Introduction to elliptic curves, The Weil pairing, the elliptic curve factoring method.

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Apply cryptanalysis in system design to protect it from various attacks.

2. Identify and investigate vulnerabilities and security threats and the mechanisms to counter them.

3. Analyse security of cryptographic algorithm against brute force attacks, birthday attacks.

4. Design cryptographic algorithms for functions and carry out their implementation. Understand the importance lattice-based cryptanalysis

Reference Books:

1. Elementary Cryptanalysis A Mathematical Approach by Abraham Sinkov, The mathematical Association of America (lnc).

2. Algorithmic Cryptanalysis, by Antoine joux, 1st Edition, CRC Press, 2009.

3. Algebraic Cryptanalysis, Bard Gregory, Springer, 2009

4. Cryptanalysis of Number Theoretic Ciphers, Sameul S. Wag staff, Chapman & Hall/CRC, 2002.

5. Cryptanalysis: A Study of Cipher and Their Solution, Helen F. Gaines,1989

22PBM17	DATA ANALYTICS FOR FRAUD DETECTION	L	T	P	C
		3	0	0	3

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. Discuss the overall process of how data analytics is applied
2. Discuss how data analytics can be used to better address and identify risks
3. Help mitigate risks from fraud and waste for our clients and organizations

Course Content:

UNIT I INTRODUCTION 9

Introduction: Defining Fraud, Anomalies versus, Fraud, Types of Fraud, Assess the Risk of Fraud, Fraud Detection, Recognizing Fraud, Data Mining versus Data Analysis and Analytics, Data Analytical Software, Anomalies versus Fraud within Data, Fraudulent Data Inclusions and Deletions

UNIT II TRANSPOSITION 9

The Data Analysis Cycle, Evaluation and Analysis, Obtaining Data Files, Performing the Audit, File Format Types, Preparation for Data Analysis, Arranging and Organizing Data, Statistics and Sampling, Descriptive Statistics, Inferential Statistics

UNIT III BRUTE FORCE CRYPTANALYSIS 9

Benford’s Law, Number Duplication Test, Z-Score, Relative Size Factor Test, Same-Same-Same Test, Same-Same-Different Test

UNIT IV ALGORITHMS FOR FUNCTIONS 9

Correlation, Trend Analysis, , GEL-1 and GEL-2 , Skimming and Cash Larceny, Billing schemes and Data Familiarization, Benford’s Law Tests, Relative Size Factor Test, Match Employee Address to Supplier data

UNIT V LATTICE BASED CRYPTANALYSIS 9

Payroll Fraud, Expense Reimbursement Schemes, Register disbursement schemes

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Formulate reasons for using data analysis to detect fraud.
2. Explain characteristics and components of the data and assess its completeness.
3. Identify known fraud symptoms and use digital analysis to identify unknown fraud symptoms.
4. Automate the detection process.
5. Verify results and understand how to prosecute fraud

Reference Books:

1. Sunder Gee, “Fraud and Fraud Detection: A Data Analytics Approach”, Wiley, 2014, ISBN: 978-1-118-77965-1

2. Bart Baesens, Veronique Van Vlasselaer, WouterVerbeke, "Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection", Wiley and SAS Business Series, 2015
3. Han, Kamber, “Data Mining Concepts and Techniques”, 3rd Ed., Morgan Kaufmann Publishers, 2012
4. Jure Leskovec, Anand Rajaraman, Jeffrey David Ullman, “Mining of Massive Datasets”, Cambridge University Press, 2nd Ed., 2014.

22PBM18	INTERNET OF THINGS	L	T	P	C
		3	0	2	4

Pre-requisite	Nil	Syllabus Version	V 0.1

Course Objectives:

1. To explore basic knowledge on computers.
2 .Learn how to solve common types of computing problems.
3. Learn basic constructs of computer programming languages .

4. Learn data types and control structures of C

Course Content:

UNIT I **INTRODUCTION** **9**

Internet of Things- Domain Specific IoTs - IoT and M2M-Sensors for IoT Applications–Structure ofIoT– IoT Map Device- IoT System Management with NETCONF-YANG

UNIT II **IoT ARCHITECTURE, GENERATIONS AND PROTOCOLS** **9**

IETF architecture for IoT - IoT reference architecture -First Generation – Description & Characteristics–Advanced Generation – Description & Characteristics–Integrated IoT Sensors – Description & Characteristics

UNIT III **IoT PROTOCOLS AND TECHNOLOGY** **9**

SCADA and RFID Protocols - BACnet Protocol -Zigbee Architecture - 6LowPAN - CoAP - Wireless Sensor Structure–Energy Storage Module–Power Management Module–RF Module–Sensing Module

UNIT IV **CLOUD ARCHITECTURE BASICS** **9**

The Cloud types; IaaS, PaaS, SaaS.- Development environments for service development; Amazon,Azure, Google Appcloud platform in industry

UNIT V **9**

IOT PROJECTS ON RASPBERRY PI

Building IOT with RASPBERRY PI- Creating the sensor project - Preparing Raspberry Pi - Clayster libraries — Hardware Interacting with the hardware - Interfacing the hardware- Internal representation of sensor values - Persisting data - External representation of sensor values - Exporting sensor data

TOTAL LECTURE PERIODS **45 Periods**

Expected Course Outcome: On completion of the course, the student is expected to
1.Demonstrate knowledge engineering principles underlying biometric systems.
2. Analyze design basic biometric system applications..

REFERENCE BOOKS

1. Arshdeep Bahga, Vijay Madisetti, Internet of Things: A hands-on approach, Universities Press, 2015

2. Dieter Uckelmann, Mark Harrison, Florian Michahelles (Eds), Architecting the Internet of Things, Springer, 2011

3. Peter Waher, 'Learning Internet of Things', Packt Publishing, 2015

4. Ovidiu Vermesan Peter Friess, 'Internet of Things — From Research and Innovation to Market Deployment', River Publishers, 2014

5. N. Ida, Sensors, Actuators and Their Interfaces: A Multidisciplinary Introduction, 2nd EditionScitech Publishers, 202014

6. Reese, G. (2009). Cloud Application Architectures: Building Applications and Infrastructure in the Cloud. Sebastopol, CA: O'Reilly Media, Inc. (2009)

Theodor F
Bartlett
Publi

22PBM19	MALWARE ANALYSIS	L	T	P	C
		3	0	2	4

Pre-requisite	Nil	Syllabus Version	V 0.1

Course Objectives:

1. To explore basic knowledge on computers.
2 .Learn how to solve common types of computing problems.
3. Learn basic constructs of computer programming languages .

4. Learn data types and control structures of C

Course Content:

UNIT I **INTRODUCTION AND BASIC ANALYSIS** **9**

Goals of Malware Analysis, AV Scanning, Hashing, Finding Strings, Packing and Obfuscation, PE file format, Static, Linked Libraries and Functions, Static Analysis tools, Virtual Machines and their usage in malware analysis, Sandboxing, Basic dynamic analysis, Malware execution, Process Monitoring, Viewing processes, Registry snapshots, Creating fake networks

UNIT II **ADVANCED STATIC ANALYSIS** **9**

X86 Architecture- Main Memory, Instructions, Opcodes and Endianness, Operands, Registers, Simple Instructions, The Stack, Conditionals, Branching, Rep Instructions, Disassembly, Global and local variables, Arithmetic operations, Loops, Function Call Conventions, C Main Method and Offsets. Portable Executable File Format, The PE File Headers and Sections, IDA Pro, Function analysis, Graphing, The Structure of a Virtual Machine, Analyzing Windows programs, Anti-static analysis techniques, obfuscation, packing, metamorphism, polymorphism

UNIT III **ADVANCED DYNAMIC ANALYSIS** **9**

Live malware analysis, dead malware analysis, analyzing traces of malware, system calls, api calls, registries, network activities. Anti-dynamic analysis techniques, VM detection techniques, Evasion techniques, , Malware Sandbox, Monitoring with Process Monitor, Packet Sniffing with Wireshark, Kernel vs. User-Mode Debugging, OllyDbg, Breakpoints, Tracing, Exception Handling, Patching

UNIT IV

MALWARE FUNCTIONALITY

Downloaders and Launchers, Backdoors, Credential Stealers, Persistence Mechanisms, Handles, Mutexes, Privilege Escalation, Covert malware launching- Launchers, Process Injection, Process Replacement, Hook Injection, Detours, APC injection, YARA rule based detection

UNIT V ANDROID MALWARE ANALYSIS

Android Malware Analysis: Android architecture, App development cycle, APKTool, APKInspector,Dex2Jar, JD-GUI, Static and Dynamic Analysis, Case studies

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1.Demonstrate knowledge engineering principles underlying biometric systems.

2. Analyze design basic biometric system applications..

REFERENCE BOOKS

22PBM20	SECURE SOFTWARE DESIGN AND DEVELOPMENT	L	T	P	C
		3	0	2	4

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. To explore basic knowledge on computers.
2 .Learn how to solve common types of computing problems.
3. Learn basic constructs of computer programming languages .

4. Learn data types and control structures of C

Course Content:

UNIT I **SECURE SOFTWARE DESIGN** **9**

Software vulnerabilities identification - software security analysis, security programming practices, fundamental software security design concepts, security testing and quality assurance.

UNIT II **ENTERPRISE APPLICATION DEVELOPMENT** **9**

Scope of enterprise software applications, Distributed N-tier software application design, Research technologies available for the presentation, Business and data tiers of an enterprise software application, Enterprise database system, Different tiers in an enterprise system, Presentsoftware solution.

UNIT III **ENTERPRISE SYSTEMS ADMINISTRATION** **9**

Directory-based server infrastructure in a heterogeneous systems environment, Server resource utilization for system reliability and availability, Administer network services (DNS/DHCP/Terminal Services/Clustering/Web/Email).

UNIT IV **ENTERPRISE NETWORK** **9**

Troubleshoot a network running multiple services management, Requirements of an enterprisenetwork, enterprise network management

9

DEFENDING APPLICATIONS

UNIT V

Handle insecure exceptions and command/SQL injection, web and mobile application defencesagainst attackers, vulnerabilities and flaws in software.

TOTAL LECTURE PERIODS **45 Periods**

Expected Course Outcome: On completion of the course, the student is expected to
1.Demonstrate knowledge engineering principles underlying biometric systems.
2. Analyze design basic biometric system applications..

REFERENCE BOOKS

Theodor R
Bartlett
Publi

1. Theodor Richardson, Charles N Thies, "Secure Software Design", Jones & Bartlett
   Publishers, 2013
2. Kenneth R. van Wyk, Mark G. Graff, Dan S. Peters, Diana L. Burley, "Enterprise Software
3. Security: A Confluence of Disciplines", Addison Wesley Professional, 1st edition, 2014
4. Loren Kohnfelder, Designing Secure Software, No Starch Press, 2021, ISBN: 9781718501928
5. Douglas A. Ashbaugh, Security Software Development Assessing and Managing Security
   Risks, Auerbach Publications, 2019, ISBN 9780367386603
6. Mouratidis, H., "Software Engineering for Secure Systems: Industrial and Research
   Perspectives",October, 2010, ISBN: 9781615208388
7. Mark S. Merkow, Lakshmikanth Raghavan, Secure and Resilient Software Development,
   June 2010, Auerbach Publications, ISBN: 9781498759618

Web Links:

22PBM21	**SECURITY ASSESSMENT AND RISK ANALYSIS**	**L**	**T**	**P**	**C**
		3	**0**	**2**	**4**

Pre-requisite	Nil	**Syllabus Version**	V 0.1

Course Objectives:

1. To explore basic knowledge on computers.
2 .Learn how to solve common types of computing problems.
3. Learn basic constructs of computer programming languages .
4. Learn data types and control structures of C

Course Content:

UNIT I SECURITY BASICS 9

Information Security Overview: critical information characteristics – availability information states – processing security Countermeasures- education, training and awareness, critical information characteristics -confidentiality - critical information characteristics – integrity, information states – storage, information states – transmission, security countermeasures-policy, procedures and practices, threats, vulnerabilities.

UNIT II THREATS AND VULNERABILITIES OF SYSTEMS & RISK MANAGEMENT 9

Threats and Vulnerabilities of Systems: Major categories of threats, threat impact areas, Countermeasures: assessments, Concepts of Risk Management: consequences, cost/benefit analysis of controls, implementation of cost-effective controls, monitoring the efficiency and effectiveness of controls , threat and vulnerability assessment.

UNIT III SECURITY PLANNING 9

Security Planning: directives and procedures for policy mechanism, Risk Management: acceptance of risk corrective actions information identification, risk analysis and/or vulnerability assessment components, risk analysis results evaluation, roles and responsibilities, Contingency Planning/Disaster Recovery: agency response procedures and continuity of operations, contingency plan components, determination of backup requirements, development of plans for recovery actions after a disruptive event, development of procedures for off-site processing, emergency destruction procedures, guidelines for determining critical and essential workload, team member responsibilities in responding to an emergency situation

UNIT IV PHYSICAL SECURITY MEASURES, PRACTICES AND PROCEDURES 9

Physical Security Measures: alarms, building construction, cabling, communications centre, environmental controls, filtered power, physical access control systems. Security Practices and Procedures: access authorization/verification, contractors, employee clearances, position sensitivity, security training and awareness, systems maintenance personnel, Administrative Security Procedural Controls: attribution, copyright protection and licensing, Auditing and Monitoring: conducting security reviews, effectiveness of security programs, investigation of security breaches, privacy review of accountability controls, review of audit trails and logs.

UNIT V OPERATIONS SECURITY 9

Operations Security (OPSEC): OPSEC surveys/OPSEC planning INFOSEC: computer security – audit, cryptography-encryption - Cryptography-strength - Case study of threat and vulnerability assessment

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1.Demonstrate knowledge engineering principles underlying biometric systems.

2. Analyze design basic biometric system applications..

REFERENCE BOOKS

1. Michael Whitman and Herbert Mattord, "Principles of Incident Response and Disaster Recovery", Thomson Course Technology, 2007, ISBN: 141883663X
2. http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf
3. Atle Refsdal, Bj rnar Solhaug, Ketil St len.Cyber-Risk Management, Springer, 2015 57
4. Martin Weiss; Michael G. Solomon, "Auditing IT Infrastructures for Compliance", Second Edition,Jones & Bartlett Learning, 2016, ISBN: 9781284090703
5. Mark Talabis and Jason Martin, "Information Security Risk Assessment Toolkit", 1st Edition, Syngres /Elsevier, 2012, ISBN: 9781597497350

22PBM22	STEGANOGRAPHY AND DIGITAL WATERMARKING	L	T	P	C
		3	0	2	4

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. To explore basic knowledge on computers.
2 .Learn how to solve common types of computing problems.
3. Learn basic constructs of computer programming languages .
4. Learn data types and control structures of C

Course Content:

UNIT I INTRODUCTION 9

Information Hiding, Steganography, and Watermarking. History of Watermarking. History of Steganography, Importance of Digital Watermarking. Importance of Steganography.

UNIT II STEGANOGRAPHY 9

Stenographic Communication, The Channel, The Building Blocks, Notation and Terminology, Information - Theoretic Foundations of Steganography, Cachin's Definition of Stenographic Security, Practical Stenographic Methods, Statistics Preserving Steganography, Model-Based Steganography, Steganalysis Scenarios, Detection, Forensic Steganalysis, The Influence of the Cover Work on Steganalysis, Some Significant Steganalysis Algorithms, LSB Embedding and theHistogram Attack

UNIT III WATERMARKING 9

Evaluating watermarking systems. Notation – Communications – Communication based models– Geometric models – Mapping messages into message vectors – Error correction coding – Detecting multi-symbol watermarks – Attacks

UNIT IV MODELS OF WATERMARKING 9

Notation, Communications, Components of Communications Systems, Classes of Transmission Channels, Secure Transmission, Communication-Based Models of Watermarking, Basic Model, Watermarking as Communications with Side Information at the Transmitter, Watermarking as Multiplexed Communications, Geometric Models of Watermarking, Distributions and Regions in Media Space, Marking Spaces, Modeling Watermark Detection by Correlation, Linear Correlation, Normalized Correlation, Correlation Coefficient, Summary

UNIT V APPLICATIONS 9

Applications of Watermarking, Broadcast Monitoring, Copyrights, Proof of Ownership, Transaction Tracking, Content Authentication, Copy Control, Device Control, Legacy Enhancement. Applications of Steganography, Steganography for Dissidents, Steganography for Criminals

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to
1. Demonstrate knowledge engineering principles underlying biometric systems.
2. Analyze design basic biometric system applications.

REFERENCE BOOKS

1. Ingemar J. Cox, Mathew L. Miller, Jefrey A. Bloom, Jesica Fridrich, Ton Kalker, “Digital Watermarking and Steganography”, Morgan Kaufmann Publishers, New York, 2008.
2. Ingemar J. Cox, Mathew L. Miller, Jefrey A. Bloom, “Digital Watermarking”, Morgan Kaufmann Publishers, New York, 2003
3. Juergen Seits, “Digital Watermarking for Digital Media”, IDEA Group Publisher, New York, 2005.
4. Jesica Fridrich, “Steganography in Digital Media: Principles, Algorithms, and Applications”, Cambridge University press, 2010.
5. Michael Arnold, Martin Schmucker, Stephen D. Wolthusen, “Techniques and Applications of Digital Watermarking and Content Protection”, Artech House, London, 2003.
6. Peter Wayner, “Disappearing Cryptography – Information Hiding: Steganography & Watermarking”, Morgan Kaufmann Publishers, New York, 2002.
7. Stefan Katzenbelser and Fabien A. P. Peticolas, “Information hiding techniques for Steganography and Digital Watermarking”, ARTECH House Publishers, January 2004.
8. Steganography, AbasChedad, VdmVerlag and Dr.Muller,“DigitalImage” Aktiengesellschaft & Co. Kg, Dec 2009.

22PBM23	BLOCKCHAIN TECHNOLOGIES	L	T	P	C
		3	0	2	4

Pre-requisite	Nil	**Syllabus Version**	V 0.1

Course Objectives:

1. This course is intended to study the basics of Blockchain technology.
2. During this course the learner will explore various aspects of Blockchain technology like application in various domains.
3. By implementing, learners will have idea about private and public Blockchain, and smart contract.

Course Content:

UNIT I **INTRODUCTION OF CRYPTOGRAPHY AND BLOCKCHAIN** **9**

Introduction to Blockchain, Blockchain Technology Mechanisms & Networks, Blockchain Origins, Objective of Blockchain, Blockchain Challenges, Transactions and Blocks, P2P Systems, Keys as Identity, Digital Signatures, Hashing, and public key cryptosystems, private vs. public Blockchain.

UNIT II BITCOIN AND CRYPTOCURRENCY **9**

Introduction to Bitcoin, The Bitcoin Network, The Bitcoin Mining Process, Mining Developments, Bitcoin Wallets, Decentralization and Hard Forks, Ethereum Virtual Machine (EVM), Merkle Tree, Double-Spend Problem, Blockchain and Digital Currency, Transactional Blocks, Impact of Blockchain Technology on Cryptocurrency.

UNIT III **INTRODUCTION TO ETHEREUM** **9**

Introduction to Ethereum, Consensus Mechanisms, Metamask Setup, Ethereum Accounts, , Transactions, Receiving Ethers, Smart Contracts.

UNIT IV **INTRODUCTION TO HYPERLEDGER AND SOLIDITY PROGRAMMING** **10**

Introduction to Hyperledger, Distributed Ledger Technology & its Challenges, Hyperledger & Distributed Ledger Technology, Hyperledger Fabric, Hyperledger Composer. Solidity - Language of Smart Contracts, Installing Solidity & Ethereum Wallet, Basics of Solidity, Layout of a Solidity Source File & Structure of Smart Contracts, General Value Types.

UNIT V **BLOCKCHAIN APPLICATIONS** **8**

Internet of Things, Medical Record Management System, Domain Name Service and Future of Blockchain, Alt Coins.

TOTAL: 45 PERIODS

LIST OF EXPERIMENTS:

1. Create a Simple Blockchain in any suitable programming language.
2. Use Geth to Implement Private Ethereum Block Chain.
3. Build Hyperledger Fabric Client Application.
4. Build Hyperledger Fabric with Smart Contract.
5. Create Case study of Block Chain being used in illegal activities in real world.

6. Using Python Libraries to develop Block Chain Application.

TOTAL: 30 PERIODS

COURSE OUTCOMES:

1. Understand and explore the working of Blockchain technology 60
2. Analyze the working of Smart Contracts
3. Understand and analyze the working of Hyperledger
4. Apply the learning of solidity to build de-centralized apps on Ethereum
5. Develop applications on Blockchain

REFERENCES:

1. Imran Bashir, “Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained”, Second Edition, Packt Publishing, 2018.
2. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction” Princeton University Press, 2016
3. Antonopoulos, Mastering Bitcoin, O’Reilly Publishing, 2014. .
4. Antonopoulos and G. Wood, “Mastering Ethereum: Building Smart Contracts and Dapps”, O’Reilly Publishing, 2018.
5. D. Drescher, Blockchain Basics. Apress, 2017.

22PBM24	WEB SECURITY	L	T	P	C
		3	0	2	4

Pre-requisite	Nil	**Syllabus Version**	V 0.1

Course Objectives:

1. To explore basic knowledge on computers.
2 .Learn how to solve common types of computing problems.
3. Learn basic constructs of computer programming languages.
4. Learn data types and control structures of C

Course Content:

UNIT I **WEB APPLICATION TECHNOLOGIES** **9**

Introduction – Evolution of web applications – Web application security – Core defense mechanisms – Handling user access – Handling user input – Handling attackers – Managing the application - The OWASP top ten list Web Application Technologies : Web functionality – Encoding schemes – Mapping the Application Enumerating the content and functionality – Analysing the application – Bypassing client side controls : Transmitting data via the client – Capturing user data – Handling client side data securely Input Validation, Blacklist Validation - Whitelist Validation - The Defence-in-Depth Approach - Attack Surface Reduction Rules of Thumb

UNIT II **WEB APPLICATION AUTHENTICATION AND SESSIONMANAGEMENT** **9**

Web Application Authentication : Authentication Fundamentals- Two factor and Three Factor authentication - Password Based, Built in HTTP, single sign-on Custom Authentication- Secured Password based authentication: Attacks against password, Importance of password complexity – Design flaws in authentication mechanisms – Implementation flaws in authentication mechanisms– Securing authentication Session Management: Need – Weaknesses in Session Token Generation – Weaknesses in Session Token Handling – Securing Session Management; Access Control : Access Control overview, Common vulnerabilities – attacking access controls – Securing Access Controls

UNIT III **WEB SECURITY PRINCIPLES** **9**

Web Security Principles: Origin Policy, Exceptions Cross Site Scripting, Cross site Forgery Scripting; File Security Principles: Source code Security, Forceful Browsing, Directory Traversals-Classifying and Prioritizing Threats Origin Policy

UNIT IV **WEB APPLICATION VULNERABILITY** **9**

Web Application Vulnerability: Understanding vulnerabilities in traditional client server application and web applications, client state manipulation, Cookie based attacks, SQL injection, cross domain attack (XSS/XSRF/XSSI) http header injection. SSL vulnerabilities and testing - Proper encryption use in web application - Session vulnerabilities and testing - Cross-site request forgery

9

UNIT V EXPLOITING SYSTEMS

Exploiting Systems: Path traversal - Finding and exploiting path traversal vulnerability – Preventing path traversal vulnerability – Information disclosure - Exploiting error messages – Securing compiled applications – Buffer overflow vulnerability – Integer vulnerability – Format string vulnerability

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Demonstrate knowledge engineering principles underlying biometric systems.
2. Analyze design basic biometric system applications.

REFERENCE BOOKS

1. B. Sullivan, V. Liu, and M. Howard, Web Application Security, A Beginner's Guide. New York: McGraw-Hill Education, 2011.
2. D. Stuttard and M. Pinto, The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws, 2nd ed. Indianapolis, IN: Wiley, John & Sons, 2011.
3. W. Hanqing and L. Zhao, Web Security: A Whitehat Perspective. United Kingdom: Auerbach Publishers, 2015.
4. M. Shema and J. B. Alcover, Hacking Web Apps: Detecting and Preventing Web Application Security Problems. Washington, DC, United States: Syngress Publishing, 2014.

Open Elective List

22OAE01	BIG DATA ANALYTICS	L	T	P	C
		3	0	0	3

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. To know the fundamental concepts of big data and analytics.
2. To explore tools and practices for working with big data
3. To learn about stream computing.
4. To know about the research that requires the integration of large amounts of data.

Course Content:

UNIT I INTRODUCTION TO BIG DATA 9

Evolution of Big data - Best Practices for Big data Analytics - Big data characteristics - Validating - The Promotion of the Value of Big Data - Big Data Use Cases- Characteristics of Big Data Applications -Perception and Quantification of Value -Understanding Big Data Storage - A General Overview of High-Performance Architecture - HDFS - Map Reduce and YARN - Map Reduce Programming Model

UNIT II CLUSTERING AND CLASSIFICATION 9

Advanced Analytical Theory and Methods: Overview of Clustering - K-means - Use Cases - Overview of the Method - Determining the Number of Clusters - Diagnostics - Reasons to Choose and Cautions .-Classification: Decision Trees - Overview of a Decision Tree - The General Algorithm - Decision Tree Algorithms - Evaluating a Decision Tree - Decision Trees in R - Naïve Bayes - Bayes' Theorem -Naïve Bayes Classifier.

UNIT III ASSOCIATION AND RECOMMENDATION SYSTEM 9

Advanced Analytical Theory and Methods: Association Rules - Overview - Apriori Algorithm - Evaluation of Candidate Rules - Applications of Association Rules - Finding Association& finding similarity - Recommendation System: Collaborative Recommendation- Content Based Recommendation Knowledge Based Recommendation- Hybrid Recommendation Approaches

UNIT IV STREAM MEMORY 9

Introduction to Streams Concepts – Stream Data Model and Architecture - Stream Computing, Sampling Data in a Stream – Filtering Streams – Counting Distinct Elements in a Stream – Estimatingmoments – Counting oneness in a Window – Decaying Window – Real time Analytics Platform(RTAP)applications - Case Studies - Real Time Sentiment Analysis, Stock Market Predictions. Using GraphAnalytics for Big Data: Graph Analytics

UNIT V NOSQL DATA MANAGEMENT FOR BIG DATA AND VISUALIZATION 9

NoSQL Databases : Schema-less Models‖: Increasing Flexibility for Data Manipulation-Key

Value Stores- Document Stores - Tabular Stores - Object Data Stores - Graph Databases Hive - Sharding —- Hbase — Analyzing big data with twitter - Big data for E-Commerce Big data for blogs - Review of Basic Data Analytic Methods using R

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Work with big data tools and its analysis techniques
2. Analyze data by utilizing clustering and classification algorithms
3. Learn and apply different mining algorithms and recommendation systems for large volumes ofdata
4. Perform analytics on data streams
5. Learn NoSQL databases and management.

Text Book(s):

1. Anand Rajaraman and Jeffrey David Ullman, "Mining of Massive Datasets", Cambridge UniversityPress, 2012.
2. David Loshin, "Big Data Analytics: From Strategic Planning to Enterprise Integration with Tools,Techniques, NoSQL, and Graph", Morgan Kaufmann/El sevier Publishers, 2013.

Reference Books:

1. EMC Education Services, "Data Science and Big Data Analytics: Discovering, Analyzing,Visualizing and Presenting Data", Wiley publishers, 2015.
2. Bart Baesens, "Analytics in a Big Data World: The Essential Guide to Data Science and itsApplications", Wiley Publishers, 2015.
3. Dietmar Jannach and Markus Zanker, "Recommender Systems: An Introduction", CambridgeUniversity Press, 2010.
4. Kim H. Pries and Robert Dunnigan, "Big Data Analytics: A Practical Guide for Managers " CRCPress, 2015.
5. Jimmy Lin and Chris Dyer, "Data-Intensive Text Processing with MapReduce", Synthesis Lectures on Human Language Technologies, Vol. 3, No. 1, Pages 1-177, Morgan Claypool publishers, 2010.

22OAE02	INTERNET OF THINGS AND CLOUD	L	T	P	C
		3	0	0	3

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

To understand Smart Objects and IoT Architectures
1.To learn about various IOT-related protocols
2.To build simple IoT Systems using Arduino and Raspberry Pi.
3.To understand data analytics and cloud in the context of IoT
4.To develop IoT infrastructure for popular applications

Course Content:

UNIT I FUNDAMENTALS OF IoT 9

Introduction to IoT – IoT definition – Characteristics – IoT Complete Architectural Stack – IoT enabling Technologies – IoT Challenges. Sensors and Hardware for IoT – Hardware Platforms – Arduino, Raspberry Pi, Node MCU. A Case study with any one of the boards and data acquisition from sensors.

UNIT II PROTOCOLS FOR IoT 9

Infrastructure protocol (IPV4/V6/RPL), Identification (URIs), Transport (Wifi, Lifi, BLE), Discovery, Data Protocols, Device Management Protocols. – A Case Study with MQTT/CoAP usage-IoT privacy, security and vulnerability solutions.

UNIT III CASE STUDIES/INDUSTRIAL APPLICATIONS 9

Case studies with architectural analysis: IoT applications – Smart City – Smart Water – Smart Agriculture – Smart Energy – Smart Healthcare – Smart Transportation – Smart Retail – Smart waste management.

UNIT IV CLOUD COMPUTING INTRODUCTION 9

Introduction to Cloud Computing - Service Model – Deployment Model- Virtualization Concepts – Cloud Platforms – Amazon AWS – Microsoft Azure – Google APIs.

UNIT V IoT AND CLOUD 9

IoT and the Cloud - Role of Cloud Computing in IoT - AWS Components - S3 – Lambda - AWS IoT Core -Connecting a web application to AWS IoT using MQTT- AWS IoT Examples. Security Concerns, Risk Issues, and Legal Aspects of Cloud Computing- Cloud Data Security

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Understand the various concept of the IoT and their technologies.
2.Develop IoT application using different hardware platforms
3. Implement the various IoT Protocols
4. Understand the basic principles of cloud computing.
5.Develop and deploy the IoT application into cloud environment T

Reference Books:

1. "The Internet of Things: Enabling Technologies, Platforms, and Use Cases", by Pethuru Raj and Anupama C. Raman ,CRC Press, 2017
2. Adrian McEwen, Designing the Internet of Things, Wiley,2013.
3. EMC Education Services, “Data Science and Big Data Analytics: Discovering, Analyzing, Visualizing and Presenting Data”, Wiley publishers, 2015.
4. Simon Walkowiak, “Big Data Analytics with R” PackT Publishers, 2016
5. Bart Baesens, “Analytics in a Big Data World: The Essential Guide to Data Science and its Applications”, Wiley Publishers, 2015.

22OAE03	**MEDICAL ROBOTICS**	**L**	**T**	**P**	**C**
		3	**0**	**0**	**3**

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. To explain the basic concepts of robots and types of robots
2. To discuss the designing procedure of manipulators, actuators and grippers
3. To impart knowledge on various types of sensors and power sources
4. To explore various applications of Robots in Medicine
5. To impart knowledge on wearable robots

Course Content:

UNIT I INTRODUCTION TO ROBOTICS 9

Introduction to Robotics, Overview of robot subsystems, Degrees of freedom, configurations and concept of workspace, Dynamic Stabilization

Sensors and Actuators

Sensors and controllers, Internal and external sensors, position, velocity and acceleration sensors, Proximity sensors, force sensors Pneumatic and hydraulic actuators, Stepper motor control circuits, End effectors, Various types of Grippers, PD and PID feedback actuator models

UNIT II MANIPULATORS & BASIC KINEMATICS 9

Construction of Manipulators, Manipulator Dynamic and Force Control, Electronic and pneumatic manipulator, Forward Kinematic Problems, Inverse Kinematic Problems, Solutions of Inverse Kinematic problems

Navigation and Treatment Planning

Variable speed arrangements, Path determination – Machinery vision, Ranging – Laser – Acoustic, Magnetic, fiber optic and Tactile sensor

UNIT III SURGICAL ROBOTS 9

Da Vinci Surgical System, Image guided robotic systems for focal ultrasound based surgical applications, System concept for robotic Tele-surgical system for off-pump, CABG surgery, Urologic applications, Cardiac surgery, Neuro-surgery, Pediatric and General Surgery, Gynecologic Surgery, General Surgery and Nanorobotics. Case Study

UNIT IV REHABILITATION AND ASSISTIVE ROBOTS 8

Pediatric Rehabilitation, Robotic Therapy for the Upper Extremity and Walking, Clinical-Based Gait Rehabilitation Robots, Motion Correlation and Tracking, Motion Prediction, Motion Replication. Portable Robot for Tele rehabilitation, Robotic Exoskeletons – Design considerations, Hybrid assistive limb. Case Study

9

UNIT V WEARABLE ROBOTS

Augmented Reality, Kinematics and Dynamics for Wearable Robots, Wearable Robot technology, Sensors, Actuators, Portable Energy Storage, Human–robot cognitive interaction (cHRI), Human– robot physical interaction (pHRI), Wearable Robotic Communication - case study

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Describe the configuration, applications of robots and the concept of grippers and actuators
2. Explain the functions of manipulators and basic kinematics
3. Describe the application of robots in various surgeries
4. Design and analyze the robotic systems for rehabilitation
5. Design the wearable robots

SUGGESTED ACTIVITIES:

1. Twitter Intelligence project performs tracking and analysis of the Twitter
2. Large-Scale Network Embedding as Sparse Matrix Factorization
3. Implement how Information Propagation on Twitter
4. Social Network Analysis and Visualization software application.
5. Implement the Structure of Links in Networks

Text Book(s):

1. Nagrath and Mittal, “Robotics and Control”, Tata McGraw Hill, First edition, 2003
2. Spong and Vidhyasagar, “Robot Dynamics and Control”, John Wiley and Sons, First edition, 2008
3. Fu.K.S, Gonzalez. R.C., Lee, C.S.G, “Robotics, co

Reference Books:

1. Bruno Siciliano, Oussama Khatib, Springer Handbook of Robotics, 1st Edition, Springer, 2008
2. Shane (S.Q.) Xie, Advanced Robotics for Medical Rehabilitation - Current State of the Art and Recent Advances, Springer, 2016
3. Sashi S Kommu, Rehabilitation Robotics, I-Tech Education and Publishing, 2007
4. Jose L. Pons, Wearable Robots: Biomechatronic Exoskeletons, John Wiley & Sons Ltd, England, 2008
5. Howie Choset, Kevin Lynch, Seth Hutchinson, “Principles of Robot Motion: Theory, Algorithms, and Implementations”, Prentice Hall of India, First edition, 2005
6. hilippe Coiffet, Michel Chirouze, “An Introduction to Robot Technology”, Tata McGraw Hill, First Edition, 1983
7. Jacob Rosen, Blake Hannaford & Richard M Satava, “Surgical Robotics: System Applications & Visions”, Springer 2011
8. Jocelyn Troccaz, Medical Robotics, Wiley, 2012 12. Achim Schweikard, Floris Ernst, Medical Robotics, Springer, 2015

22OAE04	EMBEDDED AUTOMATION	L	T	P	C
		3	0	0	3

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. To learn about the process involved in the design and development of real-time embedded system
2. To develop the embedded C programming skills on 8-bit microcontroller
3. To study about the interfacing mechanism of peripheral devices with 8-bit microcontrollers
4. To learn about the tools, firmware related to microcontroller programming
5. To build a home automation system

Course Content:

UNIT I INTRODUCTION TO EMBEDDED C PROGRAMMING 9

C Overview and Program Structure - C Types, Operators and Expressions - C Control Flow - C Functions and Program Structures - C Pointers And Arrays - FIFO and LIFO - C Structures - Development Tools

UNIT II AVR MICROCONTROLLER 9

ATMEGA 16 Architecture - Nonvolatile and Data Memories - Port System - Peripheral Features : Time Base, Timing Subsystem, Pulse Width Modulation, USART, SPI, Two Wire Serial Interface, ADC, Interrupts - Physical and Operating Parameters

UNIT III HARDWARE AND SOFTWARE INTERFACING WITH 8-BIT SERIES CONTROLLERS 9

Lights and Switches - Stack Operation - Implementing Combinational Logic - Expanding I/O - Interfacing Analog To Digital Convertors - Interfacing Digital To Analog Convertors - LED Displays : Seven Segment Displays, Dot Matrix Displays - LCD Displays - Driving Relays - Stepper Motor Interface - Serial EEPROM - Real Time Clock - Accessing Constants Table - Arbitrary Waveform Generation - Communication Links - System Development Tools

UNIT IV VISION SYSTEM 8

Fundamentals of Image Processing - Filtering - Morphological Operations - Feature Detection and Matching - Blurring and Sharpening - Segmentation - Thresholding - Contours - Advanced Contour Properties - Gradient - Canny Edge Detector - Object Detection - Background Subtraction

UNIT V HOME AUTOMATION 9

Home Automation - Requirements - Water Level Notifier - Electric Guard Dog - Tweeting Bird Feeder - Package Delivery Detector - Web Enabled Light Switch - Curtain Automation - Android Door Lock - Voice Controlled Home Automation - Smart Lighting - Smart Mailbox - Electricity Usage Monitor -Proximity Garage Door Opener - Vision Based Authentic Entry System

TOTAL LECTURE PERIODS 45 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. analyze the 8-bit series microcontroller architecture, features and pin details
2. write embedded C programs for embedded system application
3. design and develop real time systems using AVR microcontrollers
4. design and develop the systems based on vision mechanism
5. design and develop a real time home automation system

Text Book(s):

1. Dhananjay V. Gadre, "Programming and Customizing the AVR Microcontroller", McGraw-Hill, 2001.
2. Joe Pardue, "C Programming for Microcontrollers ", Smiley Micros, 2005.
3. Steven F. Barrett, Daniel J. Pack, "ATMEL AVR Microcontroller Primer : Programming and Interfacing", Morgan & Claypool Publishers, 2012

Reference Books:

1. Mike Riley, "Programming Your Home - Automate With Arduino, Android and Your Computer", the Pragmatic Programmers, Llc, 2012.
2. Richard Szeliski, "Computer Vision: Algorithms and Applications", Springer, 2011.
3. Kevin P. Murphy, "Machine Learning - a Probabilistic Perspective", the MIT Press Cambridge, Massachusetts, London, 2012.

Audit Course List

22AC001	ENGLISH FOR RESEARCH PAPER WRITING	L	T	P	C
		2	0	0	0

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. Teach how to improve writing skills and level of readability
2. Tell about what to write in each section
3. Summarize the skills needed when writing a Title
4. Infer the skills needed when writing the Conclusion
5. Ensure the quality of paper at very first-time submission

Course Content:

UNIT I INTRODUCTION TO RESEARCH PAPER WRITING 6

Planning and Preparation, Word Order, Breaking up long sentences, Structuring Paragraphs and Sentences, Being Concise and Removing Redundancy, Avoiding Ambiguity and Vagueness

UNIT II PRESENTATION SKILLS 6

Clarifying Who Did What, Highlighting Your Findings, Hedging and Criticizing, Paraphrasing and Plagiarism, Sections of a Paper, Abstracts, Introduction

UNIT III TITLE WRITING SKILLS 6

Key skills are needed when writing a Title, key skills are needed when writing an Abstract, key skills are needed when writing an Introduction, skills needed when writing a Review of the Literature, Methods, Results, Discussion, Conclusions, The Final Check

UNIT IV RESULT WRITING SKILLS 6

Skills are needed when writing the Methods, skills needed when writing the Results, skills are needed when writing the Discussion, skills are needed when writing the Conclusions

UNIT V VERIFICATION SKILLS 6

Useful phrases, checking Plagiarism, how to ensure paper is as good as it could possibly be the first- time submission

TOTAL LECTURE PERIODS 30 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Understand that how to improve your writing skills and level of readability
2. Learn about what to write in each section
3. Understand the skills needed when writing a Title
4. Understand the skills needed when writing the Conclusion
5. Ensure the good quality of paper at very first-time submission

Text Book(s):

1. Adrian Wallwork , English for Writing Research Papers, Springer New York Dordrecht Heidelberg London, 2011
2. Day R How to Write and Publish a Scientific Paper, Cambridge University Press 2006

Reference Books:

1. Goldbort R Writing for Science, Yale University Press (available on Google Books) 2006
2. Highman N, Handbook of Writing for the Mathematical Sciences, SIAM. Highman’s book 1998.

22AC002	DISASTER MANAGEMENT	L	T	P	C
		2	0	0	0

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. Summarize basics of disaster
2. Explain a critical understanding of key concepts in disaster risk reduction and humanitarian response.
3. Illustrate disaster risk reduction and humanitarian response policy and practice from multiple perspectives.
4. Describe an understanding of standards of humanitarian response and practical relevance in specific types of disasters and conflict situations.
5. Develop the strengths and weaknesses of disaster management approaches

Course Content:

UNIT I INTRODUCTION 6

Disaster: Definition, Factors and Significance; Difference between Hazard And Disaster; Natural and Manmade Disasters: Difference, Nature, Types and Magnitude.

UNIT II REPERCUSSIONS OF DISASTERS AND HAZARDS 6

Economic Damage, Loss of Human and Animal Life, Destruction Of Ecosystem. Natural Disasters: Earthquakes, Volcanisms, Cyclones, Tsunamis, Floods, Droughts And Famines, Landslides And Avalanches, Man-made disaster: Nuclear Reactor Meltdown, Industrial Accidents, Oil Slicks And Spills, Outbreaks Of Disease And Epidemics, War And Conflicts.

UNIT III DISASTER PRONE AREAS IN INDIA 6

Study of Seismic Zones; Areas Prone To Floods and Droughts, Landslides And Avalanches; Areas Prone To Cyclonic and Coastal Hazards with Special Reference To Tsunami; Post-Disaster Diseases and Epidemics

UNIT IV DISASTER PREPAREDNESS AND MANAGEMENT 6

Preparedness: Monitoring Of Phenomena Triggering a Disaster or Hazard; Evaluation of Risk: Application of Remote Sensing, Data from Meteorological And Other Agencies, Media Reports: Governmental and Community Preparedness.

UNIT V RISK ASSESSMENT 6

Disaster Risk: Concept and Elements, Disaster Risk Reduction, Global and National Disaster Risk Situation. Techniques of Risk Assessment, Global Co-Operation in Risk Assessment and Warning, People's Participation in Risk Assessment. Strategies for Survival

TOTAL LECTURE PERIODS 30 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Ability to summarize basics of disaster
2. Ability to explain a critical understanding of key concepts in disaster risk reduction and

humanitarian response.

3. Ability to illustrate disaster risk reduction and humanitarian response policy and practice from multiple perspectives.
4. Ability to describe an understanding of standards of humanitarian response and practical relevance in specific types of disasters and conflict situations.
5. Ability to develop the strengths and weaknesses of disaster management approaches

Text Book(s):

1. Goel S. L., Disaster Administration And Management Text And Case Studies",Deep & Deep Publication Pvt. Ltd., New Delhi,2009.
2. NishithaRai, Singh AK, "Disaster Management in India: Perspectives, issues and strategies "'NewRoyal book Company,2007.

Reference Books:

1. Sahni, Pradeep Et.Al. ," Disaster Mitigation Experiences And Reflections", Prentice Hall OfIndia, New Delhi,2001.

22AC003	CONSTITUTION OF INDIA	L	T	P	C
		2	0	0	0

Pre-requisite Nil **Syllabus Version** V 0.1

Course Objectives:

1. Understand the premises informing the twin themes of liberty and freedom from a civil rights perspective.
2. To address the growth of Indian opinion regarding modern Indian intellectuals' constitutional
3. Role and entitlement to civil and economic rights as well as the emergence of nationhood in the early years of Indian nationalism.
4. To address the role of socialism in India after the commencement of the Bolshevik Revolution 1917 And its impact on the initial drafting of the Indian Constitution.

Course Content:

UNIT I HISTORY OF MAKING OF THE INDIAN CONSTITUTION

History, Drafting Committee, (Composition & Working)

UNIT II PHILOSOPHY OF THE INDIAN CONSTITUTION

Preamble, Salient Features

UNIT III CONTOURS OF CONSTITUTIONAL RIGHTS AND DUTIES

Fundamental Rights, Right to Equality, Right to Freedom, Right against Exploitation, Right to Freedom of Religion, Cultural and Educational Rights, Right to Constitutional Remedies, Directive Principles of State Policy, Fundamental Duties.

UNIT IV ORGANS OF GOVERNANCE

Parliament, Composition, Qualifications and Disqualifications, Powers and Functions, Executive, President, Governor, Council of Ministers, Judiciary, Appointment and Transfer of Judges, Qualifications, Powers and Functions.

UNIT V LOCAL ADMINISTRATION

District's Administration head: Role and Importance, Municipalities: Introduction, Mayor and role of Elected Representative, CEO, Municipal Corporation. Pachayati raj: Introduction, PRI: Zila Panchayat. Elected officials and their roles, CEO Zila Pachayat: Position and role. Block level: Organizational Hierarchy (Different departments), Village level: Role of Elected and Appointed officials, Importance of grass root democracy.

UNIT VI ELECTION COMMISSION

Election Commission: Role and Functioning. Chief Election Commissioner and Election Commissioners - Institute and Bodies for the welfare of SC/ST/OBC and women.

TOTAL LECTURE PERIODS 30 Periods

Expected Course Outcome: On completion of the course, the student is expected to

1. Discuss the growth of the demand for civil rights in India for the bulk of Indians before

the arrival of Gandhi in Indian politics.

2. Discuss the intellectual origins of the framework of argument that informed the conceptualization of social reforms leading to revolution in India.
3. Discuss the circumstances surrounding the foundation of the Congress Socialist Party [CSP] under the leadership of Jawaharlal Nehru and the eventual failure of the proposal of direct elections through adult suffrage in the Indian Constitution.
4. Discuss the passage of the Hindu Code Bill of 1956.

Text Book(s):

1. The Constitution of India, 1950(Bare Act), Government Publication.
2. Dr.S.N.Busi, Dr.B. R.Ambedkar framing of Indian Constitution, 1st Edition, 2015.

Reference Books:

1. M.P. Jain, Indian Constitution Law, 7th Edn., LexisNexis,2014.
2. D.D. Basu, Introduction to the Constitution of India, LexisNexis, 2015.