ANNA UNIVERSITY, CHENNAI
AFFILIATED INSTITUTIONS
M.E. BIOMETRICS AND CYBER SECURITY
REGULATIONS – 2017
CHOICE BASED CREDIT SYSTEM

PROGRAM EDUCATIONAL OBJECTIVES (PEOs)

1. To enable graduates to pursue research, or have a successful career in academia or industries associated with **M.E. Biometrics and Cyber Security**, or as entrepreneurs.

2. To provide students with strong foundational concepts and also advanced techniques and tools in order to enable them to build solutions or systems of varying complexity.

3. To prepare students to critically analyze existing literature in an area of specialization and ethically develop innovative and research oriented methodologies to solve the problems identified.

4. To enable students to pursue lifelong multidisciplinary learning as professional engineers and scientists to effectively communicate technical information, function effectively on teams, and apply bio metrics and cyber security related solutions within a global, societal, and environmental context.

5. Prepare students to critically analyze existing literature, identify the gaps in the existing literature, map the existing problems in human identification in Cyber Security and propose innovative and research oriented solutions.

PROGRAM OUTCOMES (POs)

Engineering Graduates will be able to:

1. **Engineering knowledge**: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

2. **Problem analysis**: Identify, formulate, review research literature, and analyze complex Engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

3. **Design/development of solutions**: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

4. **Conduct investigations of complex problems**: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

5. **Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
6. **The engineer and society**: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
7. **Environment and sustainability**: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
8. **Ethics**: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9. **Individual and team work**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10. **Communication**: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
11. **Project management and finance**: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
12. **Life-long learning**: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

MAPPING OF PROGRAM SPECIFIC OBJECTIVES WITH PROGRAMME OUTCOMES

A broad relation between the Program Specific Objectives and the outcomes is given in the following table

PROGRAMME EDUCATIONAL OBJECTIVES	PROGRAMME OUTCOMES											
	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
1	3	3	3	3	3	1	1	3	1	1	1	1
2	3	3	3	3	3	1	1	3	1	1	**1**	**1**
3	3	3	2	2	3	1	1	1	1	1	**1**	**1**
4	3	3	1	1	3	3	1	1	2	1	**1**	**1**
5	3	3	3	1	3	3	1	3	1	1	**1**	3

PROGRAM SPECIFIC OBJECTIVES (PSOS)

1. To analyze, design and develop computing solutions by applying foundational concepts of computer science and engineering.
2. To apply biometric principles and practices for the secure real time systems, scientific and business applications.
3. To diagnose the biometric and cyber problems and to build the system with advance solution to solve problem with cyber ethics.

Provide mapping of 1) POs to PEOs and 2) PSOs to PEOs.
Use the following marking:

Contribution 1: Reasonable 2: Significant 3: Strong

PROGRAM SPECIFIC OBJECTIVES	PROGRAMME OUTCOMES											
	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
1	3	3	3	3	3	3	1	3	3	1	1	3
2	3	3	2	3	3	3	1	2	1	1	**1**	**1**
3	3	3	3	3	3	3	1	3	1	3	**1**	**1**

MAPPING OF PROGRAMME EDUCATIONAL OBJECTIVES WITH PROGRAMME OUTCOMES:
A broad relation between the programme objective and the outcomes is given in the following table.

		COURSE TITLE	PROGRAMME OUTCOMES											
			A	B	C	D	E	F	G	H	I	J	K	L
YEAR I	SEMESTER I	Applied Probability and Statistics	√	√										
		Network Design and Programming	√	√	√		√				√			
		Advanced Data Structures and Algorithms	√	√		√								
		Biometric Systems	√	√	√	√	√	√	√	√			√	√
		Cyber Security	√	√	√	√	√	√		√			√	√
		Mobile and Pervasive Computing	√	√		√	√			√		√	√	√
		Data Structures Laboratory	√	√	√	√	√							
		Network Design and Programming Laboratory	√	√	√	√	√						√	

			COURSE TITLE	PROGRAMME OUTCOMES											
				A	B	C	D	E	F	G	H	I	J	K	L
YEAR I	SEMESTER II		Internet of Things	√	√	√	√	√			√			√	√
			Biometric Image Processing	√	√	√	√	√						√	
			Cybercrime Investigations and Digital Forensics	√	√	√	√	√			√	√		√	√
			Access Control and Identity Management Systems	√	√										
		PROFESSIONAL ELECTIVE I	Applied Cryptography	√	√	√	√								
			Machine Learning Techniques	√	√	√	√	√						√	√
			Data Mining Techniques	√	√	√	√	√							
			Context Aware Computing	√	√	√	√								
			Digital Forensics Laboratory	√	√	√	√	√	√		√	√		√	
			Biometric Image Processing Laboratory	√	√	√	√	√	√		√	√		√	

			COURSE TITLE	PROGRAMME OUTCOMES											
				A	B	C	D	E	F	G	H	I	J	K	L
			Social Network Analysis	√	√	√	√	√							
		PROFESSIONAL ELECTIVE II	Operating Systems Security	√	√	√	√								
			Trust Management in E - Commerce	√	√					√					
			Biometric Security	√	√	√	√	√							
			Cyber Security Management and Cyber Laws	√	√	√	√				√				
YEAR II	SEMESTER III	PROFESSIONAL ELECTIVE III	Steganography and Digital Watermarking	√	√	√	√	√	√		√	√			√
			Cloud Computing Technologies	√	√	√	√	√	√		√	√			√
			Energy Aware Computing	√	√			√							
			Advances in Biometrics	√	√	√	√	√							
		PROFESSIONAL ELECTIVE IV	Intrusion Detection and Prevention Systems	√	√		√	√							
			Big data Analytics	√	√	√	√	√							√
			Wireless Security	√	√						√				
			Ethical Hacking and Network Defense	√	√	√	√	√	√		√	√			
			Project Work Phase - I	√	√	√	√	√			√	√			
	SEM IV		Project Work Phase - II	√	√	√	√	√			√	√			

ANNA UNIVERSITY, CHENNAI
AFFILIATED INSTITUTIONS
M.E. BIOMETRICS AND CYBER SECURITY
REGULATIONS – 2017
CHOICE BASED CREDIT SYSTEM
CURRICULA AND SYLLABI

SEMESTER I

SL.NO	COURSE CODE	COURSE TITLE	CATEGORY	CONTACT PERIODS	L	T	P	C
THEORY								
1.	MA5160	Applied Probability and Statistics	FC	4	4	0	0	4
2.	NE5291	Network Design and Programming	PC	3	3	0	0	3
3.	CP5151	Advanced Data Structures and Algorithms	PC	4	4	0	0	4
4.	BC5101	Biometric Systems	PC	3	3	0	0	3
5.	BC5102	Cyber Security	PC	3	3	0	0	3
6.	CP5093	Mobile and Pervasive Computing	PC	3	3	0	0	3
PRACTICALS								
7.	CP5161	Data Structures Laboratory	PC	4	0	0	4	2
8.	NE5281	Network Design and Programming Laboratory	PC	4	0	0	4	2
			TOTAL	**28**	**20**	**0**	**8**	**24**

SEMESTER II

SL.NO	COURSE CODE	COURSE TITLE	CATEGORY	CONTACT PERIODS	L	T	P	C
THEORY								
1.	CP5292	Internet of Things	PC	3	3	0	0	3
2.	BC5251	Biometric Image Processing	PC	3	3	0	0	3
3.	BC5201	Cybercrime Investigations and Digital Forensics	PC	3	3	0	0	3
4.	BC5202	Access Control and Identity Management Systems	PC	3	3	0	0	3
5.		Professional Elective I	PE	3	3	0	0	3
6.		Professional Elective II	PE	3	3	0	0	3
PRACTICALS								
7.	BC5211	Digital Forensics Laboratory	PC	4	0	0	4	2
8.	BC5212	Biometric Image Processing Laboratory	PC	4	0	0	4	2
			TOTAL	**26**	**18**	**0**	**8**	**22**

SEMESTER III

SL. NO	COURSE CODE	COURSE TITLE	CATEGORY	CONTACT PERIODS	L	T	P	C
THEORY								
1.	CP5074	Social Network Analysis	PC	3	3	0	0	3
2.		Professional Elective III	PE	3	3	0	0	3
3.		Professional Elective IV	PE	3	3	0	0	3
PRACTICALS								
4.	BC5311	Project Work Phase - I	EEC	12	0	0	12	6
			TOTAL	**21**	**9**	**0**	**12**	**15**

IV SEMESTER

SL. NO	COURSE CODE	COURSE TITLE	CATEGORY	CONTACT PERIODS	L	T	P	C
PRACTICALS								
1.	BC5411	Project Work Phase - II	EEC	24	0	0	24	12
			TOTAL	**24**	**0**	**0**	**24**	**12**

TOTAL NO. OF CREDITS: 73

FOUNDATION COURSES (FC)

SL. NO	COURSE CODE	COURSE TITLE	CATEGORY	CONTACT PERIODS	L	T	P	C
1.	MA5160	Applied Probability and Statistics	FC	4	4	0	0	4

PROFESSIONAL CORE (PC)

SL. NO	COURSE CODE	COURSE TITLE	CATEGORY	CONTACT PERIODS	L	T	P	C
1.	NE5291	Network Design and Programming	PC	3	3	0	0	3
2.	CP5151	Advanced Data Structures and Algorithms	PC	4	4	0	0	4
3.	BC5101	Biometric Systems	PC	3	3	0	0	3
4.	BC5102	Cyber Security	PC	3	3	0	0	3
5.	CP5093	Mobile and Pervasive Computing	PC	3	3	0	0	3
6.	CP5161	Data Structures Laboratory	PC	4	0	0	4	2
7.	NE5281	Network Design and Programming Lab	PC	4	0	0	4	2
8.	CP5292	Internet of Things	PC	3	3	0	0	3
9.	BC5251	Biometric Image Processing	PC	3	3	0	0	3
10.	BC5201	Cybercrime Investigations and Digital Forensics	PC	3	3	0	0	3
11.	BC5202	Access Control and Identity Management Systems	PC	3	3	0	0	3
12.	BC5211	Digital Forensics Laboratory	PC	4	0	0	4	2
13.	BC5212	Biometric Image Processing Lab	PC	4	0	0	4	2
14.	CP5074	Social Network Analysis	PC	3	3	0	0	3

EMPLOYABILITY ENHANCEMENT COURSE (EEC)

SL. NO	COURSE CODE	COURSE TITLE	CATEGORY	CONTACT PERIODS	L	T	P	C
1.	BC5311	Project Work Phase – I	EEC	12	0	0	12	6
2.	BC5411	Project Work Phase – II	EEC	24	0	0	24	12

PROFESSIONAL ELECTIVES (PE)*

SEMESTER II
ELECTIVE I

SL.No	COURSE CODE	COURSE TITLE	CATEGORY	CONTACT PERIODS	L	T	P	C
1.	BC5001	Applied Cryptography	PE	3	3	0	0	3
2.	CP5191	Machine Learning Techniques	PE	3	3	0	0	3
3.	BC5002	Data Mining Techniques	PE	3	3	0	0	3
4.	MP5391	Context Aware Computing	PE	3	3	0	0	3

SEMESTER II
ELECTIVE II

SL.No	COURSE CODE	COURSE TITLE	CATEGORY	CONTACT PERIODS	L	T	P	C
1.	BC5003	Operating Systems Security	PE	3	3	0	0	3
2.	BC5004	Trust Management in E- Commerce	PE	3	3	0	0	3
3.	BC5005	Biometric Security	PE	3	3	0	0	3
4.	BC5006	Cyber Security Management and Cyber Laws	PE	3	3	0	0	3

SEMESTER III
ELECTIVE III

SL.No	COURSE CODE	COURSE TITLE	CATEGORY	CONTACT PERIODS	L	T	P	C
1.	BC5007	Steganography and Digital Watermarking	PE	3	3	0	0	3
2.	CP5092	Cloud Computing Technologies	PE	3	3	0	0	3
3.	IF5091	Energy Aware Computing	PE	3	3	0	0	3
4.	BC5008	Advances in Biometrics	PE	3	3	0	0	3

SEMESTER III
ELECTIVE IV

SL.No	COURSE CODE	COURSE TITLE	CATEGORY	CONTACT PERIODS	L	T	P	C
1.	BC5009	Intrusion Detection and Prevention Systems	PE	3	3	0	0	3
2.	CP5293	Big Data Analytics	PE	3	3	0	0	3
3.	BC5010	Wireless Security	PE	3	3	0	0	3
4.	BC5011	Ethical Hacking and Network Defence	PE	3	3	0	0	3

MA5160 APPLIED PROBABILITY AND STATISTICS L T P C
4 0 0 4

OBJECTIVES:

This course is designed to provide the solid foundation on topics in applied probability and various statistical methods which form the basis for many other areas in the mathematical sciences including statistics, modern optimization methods and risk modeling. It is framed to address the issues and the principles of estimation theory, testing of hypothesis and multivariate analysis.

UNIT I PROBABILITY AND RANDOM VARIABLES 12

Probability – Axioms of probability – Conditional probability – Baye's theorem - Random variables - Probability function – Moments – Moment generating functions and their properties – Binomial, Poisson, Geometric, Uniform, Exponential, Gamma and Normal distributions – Function of a random variable.

UNIT II TWO DIMENSIONAL RANDOM VARIABLES 12

Joint distributions – Marginal and conditional distributions – Functions of two dimensional random variables – Regression curve – Correlation.

UNIT III ESTIMATION THEORY 12

Unbiased estimators – Method of moments – Maximum likelihood estimation - Curve fitting by principle of least squares – Regression lines.

UNIT IV 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 V MULTIVARIATE ANALYSIS 12

Random vectors and matrices – Mean vectors and covariance matrices – Multivariate normal density and its properties – Principal components - Population principal components – Principal components from standardized variables

TOTAL : 60 PERIODS

OUTCOMES :

After completing this course, students should demonstrate competency in the following topics:

- Basic probability axioms and rules and the moments of discrete and continuous random variables.
- Consistency, efficiency and unbiasedness of estimators, method of maximum likelihood estimation and Central Limit Theorem.
- Use statistical tests in testing hypotheses on data.
- Perform exploratory analysis of multivariate data, such as multivariate normal density, calculating descriptive statistics, testing for multivariate normality.

The students should have the ability to use the appropriate and relevant, fundamental and applied mathematical and statistical knowledge, methodologies and modern computational tools.

REFERENCES:

1. Devore, J. L., “Probability and Statistics for Engineering and the Sciences”, 8th Edition, Cengage Learning, 2014.
2. Dallas E. Johnson, “Applied Multivariate Methods for Data Analysis”, Thomson and Duxbury press, 1998.
3. Gupta S.C. and Kapoor V.K.,” Fundamentals of Mathematical Statistics”, Sultan and Sons, New Delhi, 2001.
4. Johnson, R.A., Miller, I and Freund J., "Miller and Freund’s Probability and Statistics for Engineers ", Pearson Education, Asia, 8th Edition, 2015.
5. Richard A. Johnson and Dean W. Wichern, “Applied Multivariate Statistical Analysis”, 5th Edition, Pearson Education, Asia, 2002.

NE5291 NETWORK DESIGN AND PROGRAMMING L T P C
3 0 0 3

OBJECTIVES:

- To understand the basic networking principles
- To explore various networking devices and protocols required for network design and
- management
- To study two novel networking technologies: SDN and DTN
- To learn network programming in UNIX C

UNIT I NETWORKING PRINCIPLES 9

Advanced multiplexing – Code Division Multiplexing, DWDM and OFDM – Shared media networks – Collision detection and collision avoidance, Hidden and Exposed Terminals – Switched networks – Datagrams, Virtual circuits, Cell switching and Label switching – Wireless Networks – Infrastructure based, ad hoc and hybrid – End to end semantics – Connectionless, Connection oriented, Wireless Scenarios –Applications, Quality of Service – End to end level and network level solutions.

UNIT II PHYSICAL NETWORK DESIGN 9

LAN cabling topologies – Ethernet Switches – High speed and Gigabit and 10Gbps – Building cabling topologies and Campus cabling topologies – Routers, Firewalls and L3 switches –Remote Access Technologies and Devices – Modems and DSLs – SLIP and PPP - WAN Design and Enterprise Networks – Core networks, distribution networks and access networks

UNIT III LOGICAL DESIGN AND MANAGEMENT 9

IPv4 and IPv6 Dynamic Addressing –Hierarchical routing – VLSMand CIDR – Transition from IPv4 to IPv6 – NAT and DHCP – Static and Dynamic routes – RIP, OSPF and BGP – VPN –RMON and SNMP.

UNIT IV INNOVATIVE NETWORKS 9

Software Defined Networks – Evolution of switches and control planes – Centralized and distributed data and control planes – OpenFlow and SDN Controllers – Network Function Virtualization – Needs of the Data Centres – SDN solutions for data centres - Delay Tolerant Networks – Overlay architecture – Bundle Protocol – Opportunistic routing and Epidemic routing

UNIT V NETWORK PROGRAMMING IN UNIX C 9

Socket address structures – Byte ordering and byte manipulation functions – Elementary TCP sockets – socket, connect, bind, listen, accept and close functions – TCP client and server – Elementary UDP sockets –recvfrom and sendto functions , connect function with UDP – Raw sockets – Client-server design alternatives – Iterative and Concurrent servers.

TOTAL: 45 PERIODS

OUTCOMES:

After studying this course, the student should be able to

- Apply the networking principles to design a network
- Apply SDN in computing paradigms like Cloud Computing and Internet of Things
- Configure the networking devices and protocols
- Develop network applications in various platforms

REFERENCES:

1. Larry Peterson and Bruce Davie, “Computer Networks: A Systems Approach”, 5th edition, Morgan Kauffman, 2011
2. ParitoshPuri, M.P.Singh,”Asurvey paper on routing in delay tolerant networks”, International Conference on Information and Computer Networks (ISCON), 2013, DOI:10.1109/ICISCON 2013.6524206
3. Paul Goransson, Chuck Black, “Software Defined Networks: A Comprehensive Approach”, Morgan Kauffman, 2014
4. W.Richard Stevens, Bill Fenner and Andrew M Rudoff, “Unix Network Programming: The Sockets Networking API: Volume 1”, 3rd Edition,Addison Wesley, 2003
5. Ying Dar Lin, Ren-Hung Hwang and Fred Baker, “Computer Networks: An Open Source Approach”, McGraw Hill, 2011

CP5151 ADVANCED DATA STRUCTURES AND ALGORITHMS L T P C

4 0 0 4

OBJECTIVES:

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

UNIT I ROLE OF ALGORITHMS IN COMPUTING 12

Algorithms – Algorithms as a Technology- Insertion Sort – Analyzing Algorithms – Designing Algorithms- Growth of Functions: Asymptotic Notation – Standard Notations and Common Functions- Recurrences: The Substitution Method – The Recursion-Tree Method

UNIT II HIERARCHICAL DATA STRUCTURES 12

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- Fibonacci Heaps: structure – Mergeable-heap operations- Decreasing a key and deleting a node-Bounding the maximum degree.

UNIT III GRAPHS 12

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; All-Pairs Shortest Paths: Shortest Paths and Matrix Multiplication – The Floyd-Warshall Algorithm;

UNIT IV ALGORITHM DESIGN TECHNIQUES 12

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

UNIT V NP COMPLETE AND NP HARD 12

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

TOTAL: 60 PERIODS

OUTCOMES:

Upon the completion of the course the student should be able to

- Design data structures and algorithms to solve computing problems.
- Design algorithms using graph structure and various string matching algorithms to solve real-life problems.
- Apply suitable design strategy for problem solving

REFERENCES:

1. Alfred V. Aho, John E. Hopcroft, Jeffrey D. Ullman, "Data Structures and Algorithms", Pearson Education, Reprint 2006.
2. Robert Sedgewick and Kevin Wayne, "ALGORITHMS", Fourth Edition, Pearson Education.
3. S.Sridhar,"Design and Analysis of Algorithms", First Edition, Oxford University Press. 2014
4. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein, "Introduction to Algorithms", Third Edition, Prentice-Hall, 2011.

BC5101	BIOMETRIC SYSTEMS	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To understand the basics of Biometrics and its functionalities
- To learn the role of biometric in the organization
- To expose the concept of IRIS and sensors
- To expose the context of Biometric Applications
- To learn to develop applications with biometric security

UNIT I INTRODUCTION 9

Person Recognition – Biometric systems –Biometric functionalities: verification, identification – Biometric systems errors - The design cycle of biometric systems – Applications of Biometric systems – Security and privacy issues.

UNIT II FINGER PRINT AND FACIAL RECOGNITION 9

FINGERPRINT : Introduction – Friction ridge pattern- finger print acquisition :sensing techniques ,image quality –Feature Extraction –matching –indexing. FACE RECOGNITION: Introduction –Image acquisition: 2D sensors ,3D sensors- Face detection- Feature extraction -matching.

UNIT III IRIS AND OTHER TRAITS 9

Design of an IRIS recognition system-IRIS segmentation- normalization – encoding and matching-IRIS quality –performance evaluation –other traits- ear detection –ear recognition –gait feature extraction and matching –challenges- hand geometry –soft biometrics.

UNIT IV BEHAVIORAL BIOMETRICS 9

Introduction –Features- classification of behavioral biometrics –properties of behavioral biometrics – signature –keystroke dynamics –voice- merits –demerits –applications- error sources-types –open issues –future trends.

UNIT V APPLICATIONS AND TRENDS 9

Application areas: surveillance applications- personal applications –design and deployment -user system interaction-operational processes – architecture –application development –design validation-disaster recovery plan-maintenance-privacy concerns.

TOTAL : 45 PERIODS

OUTCOMES:

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

- Identify the various Biometric technologies.
- Design of biometric recognition for the organization.
- Develop simple applications for privacy.
- Understand the need of biometric in the society

REFERENCES:

1. James wayman,Anil k.Jain ,Arun A.Ross ,Karthik Nandakumar, “Introduction to Biometrics”, Springer, 2011
2. John Vacca "Biometrics Technologies and Verification Systems" Elsevier 2007
3. James Wayman,Anil Jain,David MAltoni,DasioMaio(Eds) "Biometrics Systems Technology",Design and Performance Evalution.Springer 2005
4. Khalid saeed with Marcin Adamski, Tapalina Bhattasali, Mohammed K. Nammous, Piotr panasiuk, mariusz Rybnik and soharab H.Sgaikh, “New Directions in Behavioral Biometrics”, CRC Press 2017
5. Paul Reid "Biometrics For Network Security "Person Education 2004
6. Shimon K.Modi , “Biometrics in Identity Management :concepts to applications”, Artech House 2011

BC5102	CYBER SECURITY	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Students should be able to understand.
- The difference between threat, risk, attack and vulnerability.
- How threats materialize into attacks.
- Where to find information about threats, vulnerabilities and attacks.
- Typical threats, attacks and exploits and the motivations behind them.

UNIT I INTRODUCTION TO CYBER SECURITY 9

Introduction -Computer Security - Threats -Harm - Vulnerabilities - Controls - Authenticat Access Control and Cryptography - Web—User Side - Browser Attacks - Web Att Targeting Users - Obtaining User or Website Data - Email Attacks

UNIT II SECURITY IN OPERATING SYSTEM & NETWORKS 9

Security in Operating Systems - Security in the Design of Operating Systems -Rootkit - Network security attack- Threats to Network Communications - Wireless Network Security - Denial of Service - Distributed Denial-of-Service.

UNIT III DEFENCES: SECURITY COUNTERMEASURES 9

Cryptography in Network Security - Firewalls - Intrusion Detection and Prevention Systems - Network Management - Databases - Security Requirements of Databases - Reliability and Integrity - Database Disclosure - Data Mining and Big Data.

UNIT IV PRIVACY IN CYBERSPACE 9

Privacy Concepts -Privacy Principles and Policies -Authentication and Privacy - Data Mining -Privacy on the Web - Email Security - Privacy Impacts of Emerging Technologies - Where the Field Is Headed.

UNIT V MANAGEMENT AND INCIDENTS 9

Security Planning - Business Continuity Planning - Handling Incidents - Risk Analysis - Dealing with Disaster - Emerging Technologies - The Internet of Things - Economics - Electronic Voting - Cyber Warfare- Cyberspace and the Law - International Laws - Cyber crime - Cyber Warfare and Home Land Security.

TOTAL : 45 PERIODS

OUTCOMES:

- Analytical skills
- Group/team working
- Innovation/creativity
- Problem solving skills
- Research

REFERENCES:

1. Charles P. Pfleeger Shari Lawrence Pfleeger Jonathan Margulies, Security in Computing, 5th Edition , Pearson Education , 2015
2. George K.Kostopoulous, Cyber Space and Cyber Security, CRC Press, 2013.
3. Martti Lehto, Pekka Neittaanmäki, Cyber Security: Analytics, Technology and Automation edited, Springer International Publishing Switzerland 2015
4. Nelson Phillips and Enfinger Steuart, “Computer Forensics and Investigations”, Cengage Learning, New Delhi, 2009.

CP5093	MOBILE AND PERVASIVE COMPUTING	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To learn the basic architecture and concepts till Third Generation Communication systems
- To understand the latest 4G Telecommunication System Principles.
- To introduce the broad perspective of pervasive concepts and management
- To Explore the HCI in Pervasive environment
- Apply the pervasive concepts in mobile environment

UNIT I INTRODUCTION 9

History – Wireless communications: GSM – DECT – TETRA – UMTS – IMT – 2000 – Blue tooth, WiFi, WiMAX, 3G ,WATM.- Mobile IP protocols -WAP push architecture-Wml scripts and applications. Data networks – SMS – GPRS – EDGE – Hybrid Wireless100 Networks – ATM – Wireless ATM.

UNIT II OVERVIEW OF A MODERN 4G TELECOMMUNICATIONS SYSTEM 9

Introduction. LTE-A System Architecture. LTE RAN. OFDM Air Interface. Evolved Packet Core. LTE Requirements. LTE-Advanced. LTE-A in Release. OFDMA – Introduction. OFDM Principles. LTE Uplink—SC-FDMA. Summary of OFDMA.

UNIT III PERVASIVE CONCEPTS AND ELEMENTS 9

Technology Trend Overview - Pervasive Computing: Concepts - Challenges - Middleware - Context Awareness - Resource Management - Human–Computer Interaction - Pervasive Transaction Processing - Infrastructure and Devices - Wireless Networks - Middleware for Pervasive Computing Systems - Resource Management - User Tracking- Context Management -Service Management - Data Management - Security Management - Pervasive Computing Environments - Smart Car Space - Intelligent Campus

UNIT IV HCI IN PERVASIVE COMPUTING 9

Prototype for Application Migration - Prototype for Multimodalities - Human–Computer Interface in Pervasive Environments - HCI Service and Interaction Migration - Context-Driven HCI Service Selection - Interaction Service Selection Overview - User Devices - Service-Oriented Middleware Support - User History and Preference - Context Manager - Local Service Matching - Global Combination - Effective Region - User Active Scope - Service Combination Selection Algorithm

UNIT V PERVASIVE MOBILE TRANSACTIONS 9

Pervasive Mobile Transactions - Introduction to Pervasive Transactions - Mobile Transaction Framework - Unavailable Transaction Service - Pervasive Transaction Processing Framework - Context-Aware Pervasive Transaction Model - Context Model for Pervasive Transaction Processing - Context-Aware Pervasive Transaction Model - A Case of Pervasive Transactions - Dynamic Transaction Management - Context-Aware Transaction Coordination Mechanism - Coordination Algorithm for Pervasive Transactions - Participant Discovery - Formal Transaction Verification - Petri Net with Selective Transition

TOTAL : 45 PERIODS

OUTCOMES:

Upon completion of this course the students should be able to:

- Obtain a through understanding of Basic architecture and concepts of till Third Generation Communication systems.
- Explain the latest 4G Telecommunication System Principles.
- Incorporate the pervasive concepts.
- Implement the HCI in Pervasive environment.
- Work on the pervasive concepts in mobile environment.

REFERENCES:

1. Alan Colman, Jun Han, and Muhammad Ashad Kabir, Pervasive Social Computing Socially-Aware Pervasive Systems and Mobile Applications, Springer, 2016
2. J.Schiller, "Mobile Communication", Addison Wesley, 2000
3. Juha Korhonen, "Introduction to 4G Mobile Communications" , Artech House Publishers, 2014
4. Kolomvatsos, Kostas, Intelligent Technologies and Techniques for Pervasive Computing, IGI Global, 2013.
5. Minyi Guo, Jingyu Zhou, Feilong Tang, Yao Shen, " Pervasive Computing: Concepts, Technologies and Applications " CRC Press, 2016
6. M. Bala Krishna, Jaime Lloret Mauri, "Advances in Mobile Computing and Communications: Perspectives and Emerging Trends in 5G Networks", CRC 2016

CP5161	DATA STRUCTURES LABORATORY	L T P C
		0 0 4 2

OBJECTIVES:

- To acquire the knowledge of using advanced tree structures.
- To learn the usage of heap structures.
- To understand the usage of graph structures and spanning trees.

LIST OF EXPERIMENTS

Each student has to work individually on assigned lab exercises. Lab sessions could be scheduled as one contiguous four-hour session per week or two two-hour sessions per week. There will be about 15 exercises in a semester. It is recommended that all implementations are carried out in Java. If C or C++ has to be used, then the threads library will be required for concurrency. Exercises should be designed to cover the following topics:

EXPERIMENTS:

1. Implementation of Merge Sort and Quick Sort-Analysis
2. Implementation of a Binary Search Tree
3. Red-Black Tree Implementation
4. Heap Implementation
5. Fibonacci Heap Implementation
6. Graph Traversals
7. Spanning Tree Implementation
8. Shortest Path Algorithms (Dijkstra's algorithm, Bellmann Ford Algorithm)
9. Implementation of Matrix Chain Multiplication
10. Activity Selection and Huffman Coding Implementation.

TOTAL: 60 PERIODS

OUTCOMES:

Upon Completion of the course, the students will be able to:

- Design and implement basic and advanced data structures extensively.
- Design algorithms using graph structures
- Design and develop efficient algorithms with minimum complexity using design techniques.

NE5281	NETWORK DESIGN AND PROGRAMMING LABORATORY	L T P C
		0 0 4 2

OBJECTIVES:

- To practice LAN and WAN design
- To learn network programming in UNIX C and Python

NETWORK DESIGN

- Establish a LAN with a switch/hub with 3 PCs and check the connectivity and configuration
- Establish a internetwork with 2 routers and two or more LANs using static routes and check the connectivity and configuration
- Establish a dynamic routing based internetwork with 2 routers and two or more LANs using RIP/OSPF and check the connectivity and configuration
- In the internetwork created in experiment number 4, analyze the performance of various TCP variants using an FTP application

NETWORK PROGRAMMING

- Develop a C program that demonstrates inter process communication
- Develop a TCP client/server application
- Develop a UDP client/server application
- Develop an Iterative UDP server with 2 or 3 clients
- Develop a concurrent TCP server with 2 or 3 clients
- Develop a multiprotocol server with TCP and UDP and 2 clients
- Develop simple Python programs that use frequently used syntactic constructs
- Develop a Socket based application in Python
- Build client applications for major APIs (Amazon S3, Twitter etc) in Python
- Develop an application that interacts with e-mail servers in python
- Develop applications that work with remote servers using SSH, FTP etc in Python

TOTAL: 60 PERIODS

OUTCOMES:

- After completing this course the student should be able to
- Design and implement LANs and internetworks
- Develop network based applications in UNIX C and Python

CP5292 **INTERNET OF THINGS** **L T P C**
3 0 0 3

OBJECTIVES:

- To understand the fundamentals of Internet of Things
- To learn about the basics of IOT protocols
- To build a small low cost embedded system using Raspberry Pi.
- To apply the concept of Internet of Things in the real world scenario.

UNIT I INTRODUCTION TO IoT **9**

Internet of Things - Physical Design- Logical Design- IoT Enabling Technologies - IoT Levels & Deployment Templates - Domain Specific IoTs - IoT and M2M - IoT System Management with NETCONF-YANG- IoT Platforms Design Methodology

UNIT II IoT ARCHITECTURE **9**

M2M high-level ETSI architecture - IETF architecture for IoT - OGC architecture - IoT reference model - Domain model - information model - functional model - communication model - IoT reference architecture

UNIT III IoT PROTOCOLS **9**

Protocol Standardization for IoT – Efforts – M2M and WSN Protocols – SCADA and RFID Protocols – Unified Data Standards – Protocols – IEEE 802.15.4 – BACNet Protocol – Modbus– Zigbee Architecture – Network layer – 6LowPAN - CoAP - Security

UNIT IV BUILDING IoT WITH RASPBERRY PI & ARDUINO **9**

Building IOT with RASPERRY PI- IoT Systems - Logical Design using Python – IoT Physical Devices & Endpoints - IoT Device -Building blocks -Raspberry Pi -Board - Linux on Raspberry Pi - Raspberry Pi Interfaces -Programming Raspberry Pi with Python - Other IoT Platforms - Arduino.

UNIT V CASE STUDIES AND REAL-WORLD APPLICATIONS **9**

Real world design constraints - Applications - Asset management, Industrial automation, smart grid, Commercial building automation, Smart cities - participatory sensing - Data Analytics for IoT – Software & Management Tools for IoT Cloud Storage Models & Communication APIs - Cloud for IoT - Amazon Web Services for IoT.

TOTAL : 45 PERIODS

OUTCOMES:

Upon completion of this course, the students should be able to:

- Analyze various protocols for IoT
- Develop web services to access/control IoT devices.
- Design a portable IoT using Rasperry Pi
- Deploy an IoT application and connect to the cloud.
- Analyze applications of IoT in real time scenario

REFERENCES:

1. Arshdeep Bahga, Vijay Madisetti, “Internet of Things – A hands-on approach”, Universities Press, 2015
2. Dieter Uckelmann, Mark Harrison, Michahelles, Florian (Eds), “Architecting the Internet of Things”, Springer, 2011.
3. Honbo Zhou, “The Internet of Things in the Cloud: A Middleware Perspective”, CRC Press, 2012.
4. Jan Ho¨ ller, Vlasios Tsiatsis , Catherine Mulligan, Stamatis , Karnouskos, Stefan Avesand. David Boyle, "From Machine-to-Machine to the Internet of Things - Introduction to a New Age of Intelligence", Elsevier, 2014.
5. Olivier Hersent, David Boswarthick, Omar Elloumi , “The Internet of Things – Key applications and Protocols”, Wiley, 2012

BC5251	BIOMETRIC IMAGE PROCESSING	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To understand the basics of Image processing
- To model and visualize the transformation of image
- To understand the evolution of object detection
- To mine the interest of the user

UNIT I IMAGE PROCESSING FUNDAMENTALS 9

Introduction- images-sampling and frequency –Domain processing-basic image processing operations-point operators –group operations –other statistical operators –mathematical morphology

UNIT II FEATURE EXTRACTION 9

Low level Feature Extraction: Edge Detection- phase congruency- localized feature extraction-describing image motion. High Level Extraction: Thresholding and subtraction – Template matching-feature extraction by low level features- Hough transformation.

UNIT III OBJECT DETECTION 9

Object Detection- Boundary descriptors –Region descriptors –moving object detection –tracking moving features- Moving extraction and description-Texture description –classification -segmentation.

UNIT IV 3D BIOMETRIC 9

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 – security applications.

UNIT V APPLICATIONS 9

Mobile Biometrics- Biometric Application Design –Biometric Technologies issues- Biometrics in society –privacy and Biometrics –Ethics and Technology usage – human factors

TOTAL : 45 PERIODS

OUTCOMES:

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

- Understand the need of biometric in image processing
- Work on the internals Technologies of biometric
- Mine the behavior of the users in the biometric field
- Predict the possible next outcome of the image processing
- Mine the opinion of the user

REFERENCES:

1. Amine Nail -Ali and Regis Fournier "Signal and Image Processing for Biometrics" John wiley and sons,2012
2. David Zhang,Guangming, 3D Biometrics Systems and Applications" Lu, Springer 2013.
3. Julian Ashbourn, Biometrics In The New World" , Springer 2014.
4. Mark S.Nixon, Alberto S.Aguado, Feature Extraction and image processing for computer vision, Third Edition, , Elsevier 2012.
5. Scott E Baugh "Digital Image Processing and analysis" 2nd Edition CRC Press 2010
6. Tinku Acharya and Ajoy K Ray "Image Processing Principles and Applications" John wiley and sons 2005

BC5201	CYBER CRIME INVESTIGATIONS AND DIGITAL FORENSICS	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To study about cyber crime categories
- Awareness about various hacking, cracking and attacks.
- To study about various investigation strategies
- To study about various Techniques in Digital Forensics
- Basic Laws and Acts for Cyber crime

UNIT I INTRODUCTION **9**

Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime: Social Engineering, Categories of Cyber Crime, Property Cyber Crime.

UNIT II CYBER CRIME ISSUES **9**

Unauthorized Access to Computers, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation ,Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses.

UNIT III INVESTIGATION **9**

Introduction to Cyber Crime Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Hands on Case Studies. Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking.

UNIT IV DIGITAL FORENSICS: 9

Introduction to Digital Forensics, Open Source Examination Platform - Using Linux and Windows as the Host, Disk and File System Analysis, Media Analysis Concepts , Sleuth Kit, Partitioning and Disk Layouts, Special Containers, Hashing, Forensic Imaging, Internet Artifacts, Browser & Mail Artifacts, File Analysis, Image, Audio, Video, Archives, Documents, Graphical Investigation Environments, PyFLAG, Fiwalk, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition.

UNIT V LAWS AND ACTS 9

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

TOTAL :45 PERIODS

OUTCOMES:

- Knowledge about Cyber crime issues and conquer techniques
- Analysis about investigation, Encryption and Decryption Methods.
- Familiarity in Open source Digital Forensics Platform and tools

REFERENCES:

1. Bernadette H Schell, Clemens Martin, “Cybercrime”, ABC – CLIO Inc, California, 2004. Understanding Forensics in IT “, NIIT Ltd, 2005
2. Cory Altheide and Harlan Carvey, “Digital Forensics with Open Source Tools” Elsevier publication, April 2011
3. Kevin Mandia, Chris Prosise, Matt Pepe, “Incident Response and Computer Forensics “, TataMcGraw -Hill, New Delhi, 2006.
4. Nelson Phillips and Enfinger Steuart, “Computer Forensics and Investigations”, Cengage Learning, New Delhi, 2009.
5. Robert M Slade,” Software Forensics”, Tata McGraw - Hill, New Delhi, 2005.

BC5202	ACCESS CONTROL AND IDENTITY MANAGEMENT SYSTEMS	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To understand the importance of IAM with emerging mobile information society, Compliance and regulations and industry standards for Identity management
- To build the capability to assess the risks, techniques of Identity and authentication with context
- To learn and devise various access control techniques
- To study and gain knowledge on access control systems
- To do typical case studies of online applications

UNIT I INTRODUCTION 10

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 8

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), Nondiscretionary 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 : 45 PERIODS

OUTCOMES:

- Able to understand the role of IAM with emerging mobile information society , compliance and regulations and industry standards for Identity management.
- Able to learn techniques of Identity and authentication with risks assessment
- Build capability to compare various access control techniques.
- Gain knowledge on access control systems.
- Ability to carry out analysis and report strength and weakness if IAM in a given typical online applications.

REFERENCES:

1. Access Control Systems: Security, Identity Management and Trust Models Messaoud Benantar, IBM Corp, Austin, TX, USA. Library of Congress, ISBN-13: 978-0-387-00445-7 e-ISBN-13: 978-0-387-27716-5.
2. Access and Identity Management for Libraries: Controlling access to online information, Masha Garibyan, Simon McLeish and John Paschoud, Facet Publishing 2014 www.facetpublishing.co.uk.
3. Identity and Access Management GTAG , Frank Bresz, Ernst & Young LLP etal The Institute of Internal Auditors, Altamonte Springs, FL32701-4201. 2007.
4. Identity and Access Management - Digital 2020, Ray Wagner, ISSA Journal , June 2014 , www.issa.org.
5. The Definitive Guide to Security Management, Dan Sullivan, Realtimepublishers.com chapter5:Identity and Access Management http://www3.ca.com/ebook/.

BC5211	DIGITAL FORENSICS LABORATORY	L	T	P	C
		0	0	4	2

OBJECTIVES:

- Describe digital forensics and relate it to an investigative process.
- Explain the legal issues of preparing for and performing digital forensic analysis based on the investigator's position and duty.
- Perform basic digital forensics.
- Demonstrate use of digital forensics tools.
- Guide a digital forensics exercise.
- Recognize the state of the practice and the gaps in technology, policy, and legal issues.

LIST OF EXPERIMENTS

1. **Introduction to legal issues, context, and digital forensics**

   Disk Imaging and Cloning

   Use VMWare and modify device configuration in a VMWare system

   - Image a drive to a file
   - Extract individual partitions from an image file
   - Mount the image as a loopback device and read only for analysis
   - Properly sanitize a disk for cloning
   - Clone a drive versus imaging the drive
   - Verify disk and file integrity with hashing

2. **Analysis: disk structure, file systems (NTFS, EXT 2/3, HFS), and physical**

   The Sleuth Kit Tools (learn through hands-on labs)

   Live Collection.

   Download links for listed tools

   dd.exe .

   http://users.erols.com/gmgarner/forensics/userdump.exe

   http://download.microsoft.com/download/win2000srv/Utility/3.0/NT45/ENUS/Oem3sr2.zip

   fport.exe .

   http://www.foundstone.com/knowledge/proddesc/fport.html/psloggedon.exe

   http://www.sysinternals.com/Utilities/PsLoggedOn.htmlp/slist.exe

   http://www.sysinternals.com/Utilities/PsList.html

   kill.exe, auditpol.exe, dumpel.exe .

   http://www.petri.co.il/download_free_reskit_tools.htm/ntlast.exe

   http://www.foundstone.com/resources/proddesc/ntlast.htm

REFERENCES

McDougal, Monty. Live Forensics on a Windows System: Using Windows Forensic Toolchest (WFT), 2006

http://www.foolmoon.net/downloads/Live_Forensics_Using_WFT.pdf

Burdach, Mariusz. Digital forensics of the physical memory, March 2005

http://www.forensicfocus.com/index.php?name=Content&pid=57

Rose, Curtis W. Windows Live Incident Response Volatile Data Collection: Non-Disruptive User & System Memory Forensic Acquisition

http://web.archive.org/web/20040405032635/http://www.sytexif.com/whitepaper.htm

3. **Search Word Filtering from Unallocated, Slack and Swap Space**
Understand the interview process to develop an initial search list for an investigation
- Extract unallocated space from an image
- Extract slack space from an image
- Copy the swap file
- Filter out and analyze evidence from unallocated, slack and swap space using search list.
- Modify your list of search words based on the evidence you find and repeat searching as needed.

4. **Unix File Recovery – Data Unit Level**
Review of unallocated space and extracting with dls
- Interpret the file system information from the superblock
- Locate files by block number
- Recover files from unallocated blocks
- Understand contiguous and noncontiguous files
- Using the Autopsy Forensic Browser

5. **FILE RECOVERY: META DATA LAYER**
Find meta data information for evidence found in a search list
- Recover a file based on meta data
- Use the Autopsy Forensic Browser at the meta data layer
- Observe file deletion behavior at the meta data layer with different file systems

6. **FILE RECOVERY: DATA LAYER REVISITED**
- Perform searches based on file headers
- Data Carving with Foremost
- Zip password recovery

7. **ANALYSIS TECHNIQUES: KEYWORD SEARCHES, TIMELINES, HIDDEN DATA**
File Encoding and Detection
Timeline Analysis
- Use MAC time information to generate a timeline of file activity
- Interpret timeline for finding evidence.

8. **DATA MINING FOR DIGITAL FORENSICS** **8**
Encryption and Password Recovery
Steganography Detection
File Extension Renaming and Signaturing
Application Analysis.
Client and Web
Web Analysis
IRC Analysis
Network Analysis.
Collection and Analysis of Network Traffic
Wireless Network Traffic

9. **NETWORK DEVICES: ROUTERS, SWITCHES**
Analysis of Cell phones, Tablet, iPad, PDAs, etc.
Cell Phones
Tablet, iPad
PDAs

10. **INVESTIGATION OF NON-TRADITIONAL EQUIPMENT: AUTOS, WASHERS**
    MP3 Players
    Flash Media (extra credit)
    Digital Cameras

11. **BINARY CODE ANALYSIS (GUEST LECTURER: ALEX BERRY).**
    Tools for Binary Analysis
    Detection of Malicious Code
    Reverse Engineering
    Encrypted Binaries

12. **EVIDENCE: COLLECTION, PRESERVATION, TESTIMONY**
    Forensic Certifications
    Risk Analysis for Evidence Collection
    Non-IT Parents Ability to Investigate their Child's Behavior
    EnCase Forensic Toolkit
    Paraben Forensic Toolkit

13. **RESEARCH CHALLENGES.**
    Digital Life Analysis: Undergrad - Single
    Digital Life Analysis: Grad – Children
    Peer to Peer Networks
    Grid Analysis
    Public Computer Analysis
    Large Data Analysis

REFERENCES

1. Cory Altheide and Harlan Carvey, "Digital Forensics with Open Source Tools" Elsevier publication, 3rd Edition, April 2011.
2. McDougal, Monty. Live Forensics on a Windows System: Using Windows Forensic Toolchest (WFT), 2006
3. Open Source Digital Forensics: http://www.opensourceforensics.org/ http://isis.poly.edu/kulesh/forensics/list.htm

TOTAL: 60 PERIODS

OUTCOMES:

Upon Completion of the course, the students will be able to

- Practices and basic knowledge about VMware and various file system.
- Explain in Open source forensics tools
- Hands on Express in sleuth Kit Tools
- Knowledge of filter & analyse

LIST OF EQUIPMENT FOR A BATCH OF 30 STUDENTS:

(Please include only Open Source Software wherever possible.)

BC5212 BIOMETRIC IMAGE PROCESSING LABORATORY

L	T	P	C
0	0	4	2

OBJECTIVES:

- To learn to implement Image Enhancement and Segmentation.
- To learn to implement Image Acquisition and Feature Extraction -Fingerprint
- To learn to implement Image Acquisition and Feature Extraction - Face and Iris .
- To learn to implement 3D Biometric and Mobile Biometrics.

LIST OF EXPERIMENTS

1. Image Enhancement
2. Image Segmentation
3. Image Acquisition -Fingerprint
4. Feature Extraction – Fingerprint
5. Image Acquisition – Face
6. Feature Extraction – Face
7. Image Acquisition – Iris
8. Feature Extraction - Iris
9. 3D Biometric – Palmprint
10. Mobile biometrics

TOTAL: 60 PERIODS

OUTCOMES:

Upon Completion of the course, the students will be able to:

- Design and Apply Image Enhancement and Segmentation.
- Design and Apply Image Acquisition and Feature Extraction -Fingerprint
- Design and Apply Image Acquisition and Feature Extraction - Face and Iris .
- Design and Apply 3D Biometric and Mobile Biometrics.

LIST OF EQUIPMENT FOR A BATCH OF 30 STUDENTS:

(Please include only Open Source Software wherever possible.)

CP5074 SOCIAL NETWORK ANALYSIS

L	T	P	C
3	0	0	3

OBJECTIVES:

- To understand the components of the social network
- To model and visualize the social network
- To mine the users in the social network
- To understand the evolution of the social network
- To know the applications in real time systems

UNIT I INTRODUCTION **9**

Introduction to Web - Limitations of current Web – Development of Semantic Web – Emergence of the Social Web – Statistical Properties of Social Networks -Network analysis - Development of Social Network Analysis - Key concepts and measures in network analysis - Discussion networks - Blogs and online communities - Web-based networks

UNIT II MODELING AND VISUALIZATION 9

Visualizing Online Social Networks - A Taxonomy of Visualizations - Graph Representation - Centrality- Clustering - Node-Edge Diagrams - Visualizing Social Networks with Matrix-Based Representations- Node-Link Diagrams - Hybrid Representations - Modelling and aggregating social network data **–** Random Walks and their Applications –Use of Hadoop and Map Reduce - Ontological representation of social individuals and relationships.

UNIT III MINING COMMUNITIES 9

Aggregating and reasoning with social network data, Advanced Representations – Extracting evolution of Web Community from a Series of Web Archive - Detecting Communities in Social Networks - Evaluating Communities – Core Methods for Community Detection & Mining - Applications of Community Mining Algorithms - Node Classification in Social Networks.

UNIT IV EVOLUTION 9

Evolution in Social Networks – Framework - Tracing Smoothly Evolving Communities - Models and Algorithms for Social Influence Analysis - Influence Related Statistics - Social Similarity and Influence - Influence Maximization in Viral Marketing - Algorithms and Systems for Expert Location in Social Networks - Expert Location without Graph Constraints - with Score Propagation – Expert Team Formation - Link Prediction in Social Networks - Feature based Link Prediction – Bayesian Probabilistic Models - Probabilistic Relational Models

UNIT V APPLICATIONS 9

A Learning Based Approach for Real Time Emotion Classification of Tweets, A New Linguistic Approach to Assess the Opinion of Users in Social Network Environments, Explaining Scientific and Technical Emergence Forecasting, Social Network Analysis for Biometric Template Protection

TOTAL : 45 PERIODS

OUTCOMES:

Upon Completion of the course, the students will be able to

- Work on the internals components of the social network
- Model and visualize the social network
- Mine the behaviour of the users in the social network
- Predict the possible next outcome of the social network
- Apply social network in real time applications

REFERENCES:

1. Ajith Abraham, Aboul Ella Hassanien, Václav Snášel, “Computational Social Network Analysis: Trends, Tools and Research Advances”, Springer, 2012
2. Borko Furht, “Handbook of Social Network Technologies and Applications”, Springer, 1st edition, 2011
3. Charu C. Aggarwal, “Social Network Data Analytics”, Springer; 2014
4. Guandong Xu , Yanchun Zhang and Lin Li, “Web Mining and Social Networking – Techniques and applications”, Springer, 1st edition, 2012
5. Giles, Mark Smith, John Yen, “Advances in Social Network Mining and Analysis”, Springer, 2010.
6. Peter Mika, “Social Networks and the Semantic Web”, Springer, 1st edition, 2007.
7. Przemyslaw Kazienko, Nitesh Chawla,”Applications of Social Media and Social Network Analysis”, Springer,2015

BC5001 **APPLIED CRYPTOGRAPHY** **L T P C**
3 0 0 3

OBJECTIVES:

The student should be made to:

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

UNIT I INTRODUCTION & MATHEMATICAL FOUNDATION 10

Definitions – Cryptography, cryptanalysis, cryptology, classical cryptosystem- shift cipher, affine cipher, vignere 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

UNIT II BLOCK CIPHERS AND MODES OF OPERATIONS 8

Simplified DES - Data Encryption Standard-Block cipher principles-block cipher modes of operation-AES-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 SIGNATURES 9

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

UNIT V APPLICATIONS 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, Secure Electronic Transaction, Bitcoin, Email Security - PGP, Tor (The Onion Router).

TOTAL: 45 PERIODS

OUTCOMES:

Upon Completion of the course, the students should be able to:

- Compare various Cryptographic Techniques.
  Understand security issues, practices and principles in various applications.

REFERENCES:

1. Bruce Schneier and Neils Ferguson, "Practical Cryptography", First Edition, Wiley Dreamtech India Pvt Ltd, 2003.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security", Prentice Hall of India, 2002. (UNIT V).
3. Douglas R Simson "Cryptography – Theory and practice", First Edition, CRC Press, 1995.
4. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013. (UNIT I,II,III,IV).
5. https://bitcoin.org/bitcoin.pdf

6. http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF
7. https://www.youtube.com/watch?v=GwMr8Xl7JMQ
8. http://nptel.ac.in

CP5191 MACHINE LEARNING TECHNIQUES

L	T	P	C
3	0	0	3

OBJECTIVES:

- To introduce students to the basic concepts and techniques of Machine Learning.
- To have a thorough understanding of the Supervised and Unsupervised learning techniques
- To study the various probability based learning techniques
- To understand graphical models of machine learning algorithms

UNIT I INTRODUCTION **9**

Learning – Types of Machine Learning – Supervised Learning – The Brain and the Neuron – Design a Learning System – Perspectives and Issues in Machine Learning – Concept Learning Task – Concept Learning as Search – Finding a Maximally Specific Hypothesis – Version Spaces and the Candidate Elimination Algorithm – Linear Discriminants – Perceptron – Linear Separability – Linear Regression.

UNIT II LINEAR MODELS **9**

Multi-layer Perceptron – Going Forwards – Going Backwards: Back Propagation Error – Multi-layer Perceptron in Practice – Examples of using the MLP – Overview – Deriving Back-Propagation – Radial Basis Functions and Splines – Concepts – RBF Network – Curse of Dimensionality – Interpolations and Basis Functions – Support Vector Machines

UNIT III TREE AND PROBABILISTIC MODELS **9**

Learning with Trees – Decision Trees – Constructing Decision Trees – Classification and Regression Trees – Ensemble Learning – Boosting – Bagging – Different ways to Combine Classifiers – Probability and Learning – Data into Probabilities – Basic Statistics – Gaussian Mixture Models – Nearest Neighbor Methods – Unsupervised Learning – K means Algorithms – Vector Quantization – Self Organizing Feature Map

UNIT IV DIMENSIONALITY REDUCTION AND EVOLUTIONARY MODELS **9**

Dimensionality Reduction – Linear Discriminant Analysis – Principal Component Analysis – Factor Analysis – Independent Component Analysis – Locally Linear Embedding – Isomap – Least Squares Optimization – Evolutionary Learning – Genetic algorithms – Genetic Offspring: - Genetic Operators – Using Genetic Algorithms – Reinforcement Learning – Overview – Getting Lost Example – Markov Decision Process

UNIT V GRAPHICAL MODELS **9**

Markov Chain Monte Carlo Methods – Sampling – Proposal Distribution – Markov Chain Monte Carlo – Graphical Models – Bayesian Networks – Markov Random Fields – Hidden Markov Models – Tracking Methods

TOTAL: 45 PERIODS

OUTCOMES:

Upon completion of the course, the students will be able to:

- Distinguish between, supervised, unsupervised and semi-supervised learning
- Apply the apt machine learning strategy for any given problem
- Suggest supervised, unsupervised or semi-supervised learning algorithms for any given problem
- Design systems that uses the appropriate graph models of machine learning
- Modify existing machine learning algorithms to improve classification efficiency

REFERENCES:

1. Ethem Alpaydin, "Introduction to Machine Learning 3e (Adaptive Computation and Machine Learning Series)", Third Edition, MIT Press, 2014
2. Jason Bell, "Machine learning – Hands on for Developers and Technical Professionals", First Edition, Wiley, 2014
3. Peter Flach, "Machine Learning: The Art and Science of Algorithms that Make Sense of Data", First Edition, Cambridge University Press, 2012.
4. Stephen Marsland, "Machine Learning – An Algorithmic Perspective", Second Edition, Chapman and Hall/CRC Machine Learning and Pattern Recognition Series, 2014.
5. Tom M Mitchell, "Machine Learning", First Edition, McGraw Hill Education, 2013.

BC5002	DATA MINING TECHNIQUES	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Understanding of the value of data mining in solving real-world problems.
- Understanding of foundational concepts underlying data mining.
- Understanding of algorithms commonly used in data mining tools.
- Ability to apply data mining tools to real-world problems

UNIT I INTRODUCTION TO DATA MINING 9

Introduction to Data Mining – Data Mining and Machine Learning, Examples, Applications, Machine Learning and Statistics, Generalization as search, Data mining and ethics, Input-Concepts, instances and attributes, Output-Knowledge Representation.

UNIT II DATA MINING ALGORITHMS: Basic Methods 9

Inferring rudimentary rules, Statistical modeling, Constructing decision trees, Constructing rules, Mining association rules, Linear models, instance-based learning, Clustering, Credibility – Predicting performance, predicting probabilities, Cost estimation, Evaluating numeric prediction, MDL principle.

UNIT III IMPLEMENTATION 9

Decision trees, Classification rules, Extending linear models, Instance-based learning, Numeric prediction, Clustering, Bayesian networks.

UNIT IV ADVANCED DATA MINING 9

Attribute selection, Discretizing numeric attributes, transformations, Automatic data cleansing, Combining multiple models, using unlabeled data, Ensemble learning, Extensions and Applications.

UNIT V DATA MINING WORKBENCH- WEKA 9

Introduction, The Explorer, The Experimenter, Command Line Interface, Embedded machine learning, Writing New learning schemes

TOTAL : 45 PERIODS

OUTCOMES:

Upon Completion of the course, the students will be able to

- Display a comprehensive understanding of different data mining tasks and the algorithms most appropriate for addressing them.
- Evaluate models/algorithms with respect to their accuracy.
- Demonstrate capacity to perform a self-directed piece of practical work that requires the application of data mining techniques.
- Develop hypotheses based on the analysis of the results obtained and test them.
- Conceptualise a data mining solution to a practical problem.

REFERENCES:

1. David J. Hand, Heikki Mannila and Padhraic Smyth “Principles of Data Mining” (Adaptive Computation and Machine Learning), 2005
2. Ian H.Witten, Eibe Frank and Mark A. Hall,”Data Mining, Practical Machine Learning Tools and Techniques”, Third Edition, The Morgan Kaufmann Series in Data Management Systems, 2011,Elsevier Publications
3. Jiawei Han, Micheline Kamber , Jian Pei, “Data Mining: Concepts and Techniques”, Third Edition (The Morgan Kaufmann Series in Data Management Systems), 2012.
4. Margaret H Dunham, “Data Mining: Introductory and Advanced Topics”, 2003
5. Soman, K. P., Diwakar Shyam and Ajay V. “Insight Into Data Mining: Theory And Practice”, PHI, 2009.

MP5391 CONTEXT AWARE COMPUTING

L	T	P	C
3	0	0	3

OBJECTIVES:

- To understand the concept of context, representation and modeling of context, context ontology and architecture.
- To know the technologies for sensing context, location tracking services.
- To understand the need for and categories of context aware middleware systems.
- To know the UI techniques for contextual information, reconfiguration based on context, context triggered actions.
- Case study based learning on how to apply context aware computing to ubiquitous applications and context data change management.

UNIT I 10

Context Definition. Types of Context -Identity (Who), - Activity (What), Time (When), Location (Where), reasoning (Why). Representation of Context. Modeling of context: key-value, graphical, object oriented, logic based, and ontology based models. Context ontology - SOCAM architecture .Context Interpreter.

UNIT II 8

Sensing location information. Location tracking: Technologies- GPS, GSM, Assisted GPS, Wi-Fi, Ultra wideband. Metrics- accuracy, reliability, security considerations- buying new devices, coordinating service with infrastructure, Killer app. Sensing user’s state and surroundings.

UNIT III 9

Context Aware Middleware- Categorizing Middleware Taxonomy of Context-Aware Middleware. Middleware Systems: Categorization of Context-Aware Middleware Systems-Mobi PADS, Middle Where**.** Gaia meta Operating Systems-Context File System**.**

UNIT IV **9**

Proximate Selection Contextual Info -UI techniques. Automatic Contextual Reconfiguration- Add, removes, or alters components based on context. Contextual Commands- parameterize commands with context-filtered values- universal remote control. Context-triggered Actions- Expressiveness of language for rules, Accuracy of context information.

UNIT V **9**

Case study-How does context-aware computing fit in with ubicomp. What sensors, infrastructure, are necessary. Fallback condition. How to describe the context that you are in now- location, physiological state, emotional state, etc. Challenges in Implementing a Context-Aware System- How to represent context internally- Storage, Data structures and algorithms. How frequently does the system need to be updated on context changes- How often to poll? How often to change behavior.

TOTAL: 45 PERIODS

OUTCOMES :

- Understand the concept of context, representation and modeling of context, context ontology and architecture.
- Gain knowledge on communication the technologies for sensing and transporting context data and location tracking services.
- Understand the categories of context aware middleware systems to realize mobile services
- Gain knowledge on UI techniques for contextual information, reconfiguration and context triggered actions
- Able to apply context aware computing to ubiquitous applications and implement context data change management.

REFERENCES:

1. Anind K Dey, "Context Aware Computing", IEEE 2009.
2. Bill Schilit, Norman Adams,and Roy Want, Context-Aware Computing Applications, IEEE Mobile Computing Systems and Applications, 1994.
3. Satyanarayana, "Challenges in Implementing a Context-Aware System", CMU,2001
4. Satyanarayanan, "Pervasive Computing: Vision And Challenges", IEEE Personal Communications, 2001.
5. T.J.Watson Tom Erickson, "Context-aware computing", IBM Research Center, 2002.
6. Waltenegus Dargie, "Context Aware Computing and Self Managing Systems", CRC Press, 2009.

BC5003	OPERATING SYSTEMS SECURITY	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Study the basic concepts and functions of operating systems.
- Understand the structure and functions of OS.
- Learn about Processes and memory management schemes.
- Study I/O management and File systems.
- To gain insight on to the Protection, Security issues

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 : 45 PERIODS

OUTCOMES:

- Compare and contrast various memory management schemes.
- Design and Implement a prototype file systems.
- Discuss the various synchronization, and memory management issues.
- Demonstrate the Mutual exclusion, Deadlock detection and agreement protocols of Distributed operating system.
- Discuss the various Security issues.

REFERENCES:

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.

http://nptel.ac.in/.

BC5004	TRUST MANAGEMENT IN E-COMMERCE	L	T	P	C
		3	0	0	3

OBJECTIVES:

Study and Basic Knowledge about

- Ecommerce business models and Digital Payments systems
- Knowledge about Ecommerce security Environment
- To study about Ecommerce mechanisms and trusted computing Platform.

UNIT I INTRODUCTION TO E-COMMERCE 9

Introduction to E-Commerce – Network and E-Commerce – Types of E-Commerce – Ecommerce Business Models: B2C, B2B, C2C, P2P and M-commerce business models – Ecommerce Payment systems: Types of payment system – Credit card E-Commerce -transactions– B2C E-Commerce Digital payment systems – B2B payment system.

UNIT II E-COMMERCE SECURITY 9

Security and Encryption: E-Commerce Security Environment – Security threats in E-Commerce environment – Policies, Procedures and laws.

UNIT III TRUST IN E-COMMERCE 9

Inter-organizational trust in E-Commerce: Need – Trading partner trust – Perceived benefits and risks of E-Commerce – Technology trust mechanism in E-Commerce – Perspectives of organizational, economic and political theories of inter-organizational trust – Conceptual model of inter-organizational trust in E-Commerce participation.

UNIT IV TRUSTED COMPUTING PLATFORM 9

Introduction to trusted computing platform: Overview – Usage Scenarios – Key components of trusted platform – Trust mechanisms in a trusted platform.

UNIT V TRUST MODELS 9

Trusted platforms for organizations and individuals – Trust models and the E-Commerce domain.

TOTAL : 45 PERIODS

OUTCOMES:

- Awareness about threats in Ecommerce.
- Knowledge about B2C,B2B,C2C,Business models
- Deep Knowledge about Types of Payment

REFERENCES:

1. Kenneth C. Laudon and Carol Guercio Trave, “E-Commerce Business Technology Society”, 12th Edition Pearson Education, 2016.
2. Pauline Ratnasingam, “Inter-Organizational Trust for Business-to-Business E- Commerce”, IRM Press, 2005.
3. Siani Pearson, et al, “Trusted Computing Platforms: TCPA Technology in Context” Prentice Hall PTR, 2002.

BC5005	BIOMETRIC SECURITY	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To understand the fundamentals of biometric security
- To acquire knowledge on standard algorithms and protocols used to provide confidentiality, integrity and authenticity.
- To understand the various key distribution and management strategies.
- To understand how to deploy encryption techniques to secure data using biometric
- To design security applications in the field of Information technology

UNIT I ATTACKS IN BIOMETRIC 9

Adversary attacks-attacks at the user Interface-Attacks on the biometric processing, Attacks on template database –system security analysis – spoofing and mimicry attacks

UNIT II BIOMETRIC AUTHENTICATION PROTOCOLS 9

Introduction-biometric based secure cryptographic protocols – biometrics based cryptographic key Regeneration and sharing – Biometrics based session key generation and sharing protocol – performance evaluation strategies.

UNIT III BIOMETRIC CRYPTOGRAPHY 9

Protection of biometric data –biometric data shuffling scheme- experimental results –security analysis - cryptographic key Reservation - cryptographic key with biometrics-Revocability in key generation system-Adaptations of Generalized key Regeneration scheme –IRIS Biometrics –Face Biometrics –Extension of Key Regeneration scheme.

UNIT IV BIOMETRIC DATA PROTECTION 9

Biometric data – Concept of personal data – Data protection and privacy – Security criteria for Biometric system – Adoption of security – Revocation procedures – Security and organizational aspects of biometric system.

UNIT V BIOMETRIC MULTI MODAL AND APPLICATIONS 9

Integration – Multiple traits – Multiple snapshots – Score fusion methods – Applications – Board Security – Identification cards – Biometrics on smart cards – Overview of local and global structure – Mechanism for on card comparison – Off card and On card alignment – Smart textile sensors – Bio signals – Biometrics and intelligence services.

TOTAL : 45 PERIODS

OUTCOMES:

Upon Completion of the course, the students will be able to

- Implement basic security algorithms required by the biometric system.
- Analyze the vulnerabilities in biometric system and hence be able to design a security Solution.
- Analyze the possible security attacks in complex real time systems and their effective Countermeasures
- Identify the security issues in the network and resolve it.
- Formulate research problems in the biometric security field

REFERENCES:

1. David Check Ling Ngo,Andrew Beng Jin Teoh,Jiankun Hu "Biometric Security" Cambridge Scholars,2015
2. Els. J.Kindt, “Privacy and data protection issues of Biometric Applications “, Springer,2013.
3. Eliza Yinzi Du, “Biometrics from fiction to practice”, Panstandford Publishers 2012.
4. James wayman, “Introduction to Biometrics”, Springer 2011
5. Liangwang,Xin Geng "Behavioral Biometrics for Human Identifications Intelligent Applications" Medical Information Science Reference, IGI Global 2010
6. Patrizio campisi "Security and Privacy in Biometrics" Springer 2013
7. Sanjay G.Kanade “Enhancing Information Security and Privacy”, by combining Biometrics with Cryptography, Morgan and Claypool Publishers,2012.

BC5006 CYBER SECURITY MANAGEMENT AND CYBER LAW

L	T	P	C
3	0	0	3

OBJECTIVES:

- To understand the nature of threats and cyber security management goals technology
- To understand the landscape of hacking and perimeter defense mechanisms
- To develop strategies for cyber security and protecting critical infrastructure
- To understand policies to mitigate cyber risks and digital signature
- To understand the IT Act , scheme, amendments, IPR and emerging cyber law and desired cyber ecosystem capabilities.

UNIT I **10**

Introduction- Cyberspace , Cyber Crime, Nature of Threat, Cyber security, Cyber security Policy, Mission and Vision of Cyber security Program. Cyber security management system- goals, technology categories – perimeter defense and encryption. Cyber security management framework.

UNIT II **8**

Introduction to Hacker Means, Social Engineering, Scanners, password Cracking, IP Spoofing Trojan Horses. Case study: an example of how a bank/plant was hacked. The Cyber Security Management System: Policy - Password Management, Anti-Virus, Incident Handling, Backup and Recovery, Proprietary Information. Technology - Perimeter Defense, Types of Network Security Devices - Firewalls, Intrusion Detection Systems, Content Filtering, Virtual Private Networks, Encryption.

UNIT III **9**

STRATEGIES FOR CYBER SECURITY -Creating a Secure Cyber, Types of Attacks , Comparison of Attacks , Creating an Assurance Framework, Encouraging Open Standards, Strengthening the Regulatory framework, Creating Mechanisms for IT Security, Securing E-Governance Services, Protecting Critical Information Infrastructure.

UNIT IV **9**

POLICIES TO MITIGATE CYBER RISK -Promotion of R&D in Cyber security, Reducing Supply Chain Risks, Mitigate Risks through Human Resource Development, Creating Cyber security Awareness, Information sharing Implementing a Cyber security Framework. SIGNATURES -Digital Signature ,Electronic Signature, Digital Signature to Electronic.

UNIT V **9**

Information Technology Act: Salient Features, Scheme, Application of the I.T. Act ,Amendments I.T. Act , Offences,Compounding of Offences. INTELLECTUAL PROPERTY RIGHTS: Types of Intellectual Property Rights, Intellectual Property Rights in India, Intellectual Property in Cyber Space. Emerging Trends of Cyber Law. Desired Cyber Ecosystem Capabilities.

TOTAL : 45 PERIODS

OUTCOMES:

- Gain knowledge on the nature of threats and cyber security management goals and framework
- Knowledge on the landscape of hacking and perimeter defense mechanisms
- Ability to differentiate and integrate strategies for cyber security and protecting critical infrastructure
- Able to understand policies to mitigate cyber risks
- Knowledge on IT Act, and amendments, copy rights, IPR and cyber law to deal with offenses.

REFERENCES:

1. Cyber Security Best Practices Guide For IIROC Dealers Members, Canada.
2. NIST Cyber security Framework, Version 1.0, 2014
3. CGI, “Cyber security in Modern Critical Infrastructure Environments,” 2014
4. John H. Dexter , “The Cyber Security Management System – A Conceptual Mapping”, The SANs Institute, 2002.
5. Peter Trim and Yang-Im Lee, “Cyber Security Management- A Governance, Risk and Compliance Framework”, Gower Publishing, England 2014
6. Stuart Broderick J , Cyber Security Program, Cisco Security Solutions, June 2016
7. www.Tutorialspoint.com,Information Security and Cyber Law,Tutorials Point (I) Pvt. Ltd, 2015

BC5007 STEGANOGRAPHY AND DIGITAL WATERMARKING L T P C
3 0 0 3

OBJECTIVES:

- To provide the importance of digital watermarking and Steganography
- To discuss the properties of watermarking and steganography systems
- To discuss the different models of watermarking and steganography
- To understand the various evaluation metrics
- To examine various applications of watermarking and steganography

UNIT I INTRODUCTION 5

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

UNIT II STEGANOGRAPHY 12

Steganographic Communication, The Channel, The BuildingBlocks, Notation and Terminology, Information - Theoretic Foundations of Steganography, Cachin’s Definition of Steganographic Security, Practical Steganographic Methods, StatisticsPreserving Steganography, Model-Based Steganography, Steganalysis Scenarios, Detection, Forensic Steganalysis, The Influence of the Cover Work on Steganalysis, Some Significant Steganalysis Algorithms, LSB Embedding and the Histogram Attack.

UNITI III WATERMARKING 7

Properties – 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 12

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: 45 PERIODS

OUTCOMES:

Upon Completion of the course, the students will be able to

- Discuss the need for watermarking and steganography
- Distinguish between watermarking and steganography
- Elaborate on the various models of watermarking and steganography.
- Point out various steganalysis algorithms.
- Show how watermarking and steganography can be applied to various applications and evaluate them.

REFERENCES:

1. Ingemar J. Cox, Mathew L. Miler, Jefrey A. Blom, Jesica Fridrich, Ton Kalker, "Digital Watermarking and Steganography", Morgan Kaufmann Publishers, New York, 2008.
2. Ingemar J. Cox, Mathew L. Miler, Jefrey A. Blom, "Digital Watermarking", Morgan Kaufmann Publishers, New York, 2003
3. Ingemar Cox, Mathew Miler,Jefrey Blom,Jesica Fridrich and Ton Kalker, "Digital Watermarking and Steganography", Morgan Kaufmann Publishers, Nov 2007.
4. Juergen Seits, "Digital Watermarking for Digital Media", IDEA Group Publisher, New York, 2005.
5. Jesica Fridrich, "Steganography in Digital Media: Principles, Algorithms, and Applications", Cambridge University press, 2010.
6. Michael Arnold, Martin Schmucker, Stephen D. Wolthusen, "Techniques and Aplications of Digital Watermarking and Contest Protection", Artech House, London, 2003.
7. Peter Wayner, "Disapearing Cryptography – Information Hiding: Steganography & Watermarking", Morgan Kaufmann Publishers, New York, 2002.
8. Stefan Katzenbelser and Fabien A. P. Peticolas, "Information hiding techniques for Steganography and Digital Watermarking", ARTECH House Publishers, January 2004.
9. Steganography, Ab as Chedad, Vdm Verlag and Dr. Muler, "Digital Image" Aktienge sels chaft & Co. Kg, Dec 2009.

CP5092	CLOUD COMPUTING TECHNOLOGIES	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To understand the concepts of virtualization and virtual machines
- To gain expertise in server, network and storage virtualization.
- To understand and deploy practical virtualization solutions and enterprise solutions
- To gain knowledge on the concept of virtualization that is fundamental to cloud computing
- To understand the various issues in cloud computing
- To be able to set up a private cloud
- To understand the security issues in the grid and the cloud environment

UNIT I VIRTUALIZATION 9

Basics of Virtual Machines - Process Virtual Machines – System Virtual Machines –Emulation – Interpretation – Binary Translation - Taxonomy of Virtual Machines. Virtualization –Management Virtualization –– Hardware Maximization – Architectures – Virtualization Management – Storage Virtualization – Network Virtualization

UNIT II VIRTUALIZATION INFRASTRUCTURE 9

Comprehensive Analysis – Resource Pool – Testing Environment –Server Virtualization – Virtual Workloads – Provision Virtual Machines – Desktop Virtualization – Application Virtualization - Implementation levels of virtualization – virtualization structure – virtualization of CPU, Memory and I/O devices – virtual clusters and Resource Management – Virtualization for data center automation.

UNIT III CLOUD PLATFORM ARCHITECTURE 9

Cloud deployment models: public, private, hybrid, community – Categories of cloud computing: Everything as a service: Infrastructure, platform, software- A Generic Cloud Architecture Design – Layered cloud Architectural Development – Virtualization Support and Disaster Recovery – Architectural Design Challenges - Public Cloud Platforms : GAE,AWS – Inter-cloud Resource Management

UNIT IV PROGRAMMING MODEL 9

Introduction to Hadoop Framework - Mapreduce, Input splitting, map and reduce functions, specifying input and output parameters, configuring and running a job –Developing Map Reduce Applications - Design of Hadoop file system –Setting up Hadoop Cluster - Cloud Software Environments - Eucalyptus, Open Nebula, Open Stack, Nimbus

UNIT V CLOUD SECURITY 9

Cloud Infrastructure security: network, host and application level – aspects of data security, provider data and its security, Identity and access management architecture, IAM practices in the cloud, SaaS, PaaS, IaaS availability in the cloud - Key privacy issues in the cloud –Cloud Security and Trust Management

TOTAL : 45 PERIODS

OUTCOMES:

Upon completion of this course, the students should be able to:

- Employ the concepts of storage virtualization, network virtualization and its management
- Apply the concept of virtualization in the cloud computing
- Identify the architecture, infrastructure and delivery models of cloud computing
- Develop services using Cloud computing
- Apply the security models in the cloud environment

REFERENCES:

1. Danielle Ruest, Nelson Ruest, “Virtualization: A Beginner"s Guide”, McGraw-Hill Osborne Media, 2009.
2. Jim Smith, Ravi Nair , "Virtual Machines: Versatile Platforms for Systems and Processes", Elsevier/Morgan Kaufmann, 2005
3. John W.Rittinghouse and James F.Ransome, "Cloud Computing: Implementation, Management, and Security", CRC Press, 2010.
4. Kai Hwang, Geoffrey C Fox, Jack G Dongarra, "Distributed and Cloud Computing, From Parallel Processing to the Internet of Things", Morgan Kaufmann Publishers, 2012.
5. Tim Mather, Subra Kumaraswamy, and Shahed Latif ,"Cloud Security and Privacy", O’Reilly Media, Inc.,2009.
6. Toby Velte, Anthony Velte, Robert Elsenpeter, "Cloud Computing, A Practical Approach", McGraw-Hill Osborne Media, 2009.
7. Tom White, "Hadoop: The Definitive Guide", Yahoo Press, 2012.

IF5091	ENERGY AWARE COMPUTING	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To understand the fundamentals of Energy Efficient Computing
- To understand the concept of Energy Efficient Storage Systems
- To introduce the various types of scheduling algorithms in energy efficient computing
- To introduce the concept of Green Networking
- To study Energy Aware Computing Applications

UNIT I INTRODUCTION 9

Subreshold Computing – Energy Efficient Network-on-Chip Architectures for Multi-Core Systems-Energy-Efficient MIPS CPU Core with Fine-Grained Run-Time Power Gating – Case Study : Geyser.

UNIT II ENERGY EFFICIENT STORAGE 9

Power-Efficient Strategies for Storage Systems-Energy-Saving Techniques for Disk Storage Systems -Thermal and Power-Aware Task Scheduling and Data Placement for Storage Centric Data centres - Energy-Saving Techniques for Disk Storage Systems.

UNIT III ENERGY EFFCIENT SCHEDULING ALGORITHMS 9

Algorithms and Analysis of Energy-Efficient Scheduling of Parallel Tasks- Dynamic Voltage Scaling- Speed Scaling - Memetic Algorithms for Energy-Aware Computation and Communications Optimization in Computing Clusters- Online job scheduling Algorithms.

UNIT IV INTRODUCTION TO GREEN NETWORKING 9

Power-Aware Middleware for Mobile Applications -Energy Efficiency of Voice-over-IP Systems - Intelligent Energy-Aware Networks - Green TCAM-Based Internet Routers.

UNIT V ENERGY AWARE COMPUTING APPLICATIONS 9

Energy Awareness in Video Codec Design-Overview of H.264/AVC Video Codec Design-Energy Aware Surveillance Camera -Low Power Design Challenge in Biomedical Implant Electronics

TOTAL : 45 PERIODS

OUTCOMES:

Upon Completion of the course, the students will be able to

- Design Power efficient architecture Hardware and Software
- Analyze the different types of Energy Efficient Storage systems.
- Design the algorithms for Energy Efficient Systems
- Identify the different types of Green Networking schemes in the energy efficient computing
- Explore the applications of Energy Aware Computing

REFERENCES:

1. Bob steiger wald ,Chris:Luero, Energy Aware computing, Intel Press,2012
2. Chong -Min Kyung, Sungioo yoo, Energy Aware system design Algorithms and Architecture, Springer, 2011.
3. Ishfaq Ah mad, Sanjay Ranka, Handbook of Energy Aware and Green Computing, Chapman and Hall/CRC, 2012.

BC5008 ADVANCES IN BIOMETRICS

L	T	P	C
3	0	0	3

OBJECTIVES

- Understand system requirements for biometric design
- To introduce the broad perceptive of advanced biometric technologies
- To understand the concept of Touch less Fingerprint
- To apply different methods and model as per need.
- To be able to set up a implementation of biometric system
- To understand the ethical usage of biometric system

UNIT I INTRODUCTION 9

.Overview – managing credentials – Biometric Integration – Data Dissemination – Mobile Biometrics –Biometric Techniques – Biometric Application Design- Registration process – Threshold – user interface – Hardware and Software- Technology issues – Data Management – Standards.

UNIT II TOUCHLESS FINGERPRINT 9

Touch less Fingerprint Recognition Techniques – Quality Assessment of Touch less Fingerprint Images-Computation of Touch Equivalent images – Quality Assessment of Touch Equivalent Fingerprint- Analysis of Level 1 Features and Level 2 Features in Touch less Fingerprint –Reduction of perspective and rotation Effects –Computation of synthetic Touch less Fingerprint

UNIT III IMPLEMENTATION ASPECTS 9

Ergonomic Design of Biometric Devices –Function Creep - understanding of Biometric Technology –mechanics and Engineering Design – S/W for IT Structure – H/W for IT Structure – Security vulnerabilities –Weaknesses – Strategies for increasing the adoption.

UNIT IV AUTHENTICATION 9

Basic operations –standardization – certification –web service authentication – large scale deployment – radical based approach – models –framework – rank level fusion – ammar matching technique – prologue – handwritten signature –analyzers –offline methods –online methods .

UNIT V BIOMETRIC IN SOCIETY AND ETHICAL USAGE 9

Purpose – public sector Implementation – Border Control – Responsibilities –Customer service – Government sector – Agriculture – Academic Research – Online Communications – Environmental situations – External pressure – Distractions – Implementations issues – Future Works.

TOTAL : 45 PERIODS

OUTCOMES:

Upon the students will be able to Completion of the course,

- Compare the strengths and limitations of Touch less Fingerprint
- Describe the requirements for design and implementation
- Explain the challenges in Biometric field
- To explore the characteristics of different types of Biometrics
- To analyze the strengths and limitations for development of Biometric systems

REFERENCES:

1. Julian Ashbourn, “Biometrics in the new world”, Springer 2014.
2. Patrick S. P. Wang, “Pattern Recognition, Machine Intelligence and Biometrics”, Springer Science & Business Media, 2011.
3. Ruggero Donida Labati, Vincenzo Piuri, Fabioscotti, “Touch less Fingerprint Biometrics” , CRC Press 2016.
4. Ravindra Das, “Adopting Biometric Technology: Challenges and Solutions”, CRC Press, 2016.
5. Shimon K.Modi , “Biometrics in Identity Management :concepts to applications”, Artech House 2011

BC5009	INTRUSION DETECTION AND PREVENTION SYSTEMS	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To understand the vulnerabilities and detection techniques of various attacks
- To understand the network intrusion detection & prevention mechanisms
- To understand the countermeasures of various information security attacks
- To design / make use of a typical intrusion detection system

UNIT I INTRUSION DETECTION SYSTEMS PRINCIPLES 9

History of Intrusion detection, Audit, Concept and definition , Internal and external threats to data, attacks, Key functions of IDPS technologies - Common Detection methodologies-Signature & Anomaly based Detection, Stateful protocol analysis Types of IDS, Information sources Host based information sources, Network based information sources.

UNIT II IDS TECHNOLOGIES 9

Components & Architecture-Typical components, Network Architectures Security capabilities - Information gathering capabilities, logging capabilities, detection & prevention capabilities. Intrusion Prevention Systems, Network protocol based IDS ,Hybrid IDS, Analysis schemes, thinking about intrusion. A model for intrusion analysis , techniques Responses requirement of responses, types of responses mapping responses to policy Vulnerability analysis, credential analysis non credential analysis

UNIT III NETWORK BASED IDS 9

Networking Overview-OSI layers. Components and Architecture - Typical components, Network architectures and sensor locations. Security capabilities Wireless IDPS-Wireless Networking overview-WLAN standards & components. Components Network Behavior analysis system.

UNIT IV HOST BASED IDS 9

Components and Architecture-Typical components, Network architectures, Agent locations, host architectures. Security capabilities-Logging, detection, prevention and other capabilities.Using & Integrating multiple IDPS technologies-Need for multiple IDPS technologies,Integrating different IDPS technologies-Direct & Indirect IDPS integrationo Other technologies with IDPS capabilities-Network Forensic Analysis Tool, Anti-malware technologies, Firewalls and Routers, Honeypots

UNIT V IDS TOOL : SNORT IDS 9

Introduction to Snort, Working with Snort Rules, Snort configuration, Snort with MySQL, Running Snort on Multiple Network Interfaces, Snort Modes Snort Alert Modes, Snarf with Snort, Agent development for intrusion detection, Architecture models of IDS and IPS.

TOTAL : 45 PERIODS

OUTCOMES:

Upon successful completion of this course, a student will be able to:

- Design and implement Intrusion Detection System
- Understand t classes of attacks on computer systems
- Identify various types of IDS of signature based and anomaly based techniques to solve problems related to intrusion detection and prevention.
- Employ ID&PS specific feature extraction techniques

REFERENCES:

1. Carl Endorf, Eugene Schultz and Jim Mellander " Intrusion Detection & Prevention", 1st Edition, Tata McGraw-Hill, 2006
2. Christopher Kruegel,Fredrik Valeur, Giovanni Vigna: "Intrusion Detection and Correlation Challenges and Solutions", 1st Edition,Springer, 2005.
3. Karen Scarfone, Peter Mell," Guide to Intrusion Detection and Prevention Systems (IDPS)", NIST special publication, 2007
4. Kerry J Cox , Christopher Gerg," Managing Security with Snort and IDS Tools", O′Reilly, 2007.
5. Rafeeq Rehman : " Intrusion Detection with SNORT, Apache,MySQL, PHP and ACID," 1st Edition, Prentice Hall , 2003
6. Stephen Northcutt, Judy Novak : "Network Intrusion Detection", 3rd Edition, New Riders Publishing, 2002.

CP5293 BIG DATA ANALYTICS L T P C

3 0 0 3

OBJECTIVES:

- To understand the competitive advantages of big data analytics
- To understand the big data frameworks
- To learn data analysis methods
- To learn stream computing
- To gain knowledge on Hadoop related tools such as HBase, Cassandra, Pig, and Hive for big data analytics

UNIT I INTRODUCTION TO BIG DATA 7

Big Data – Definition, Characteristic Features – Big Data Applications - Big Data vs Traditional Data - Risks of Big Data - Structure of Big Data - Challenges of Conventional Systems - Web Data – Evolution of Analytic Scalability - Evolution of Analytic Processes, Tools and methods - Analysis vs Reporting - Modern Data Analytic Tools.

UNIT II HADOOP FRAMEWORK 9

Distributed File Systems - Large-Scale FileSystem Organization – HDFS concepts - MapReduce Execution, Algorithms using MapReduce, Matrix-Vector Multiplication – Hadoop YARN

UNIT III DATA ANALYSIS 13

Statistical Methods:Regression modelling, Multivariate Analysis - Classification: SVM & Kernel Methods - Rule Mining - Cluster Analysis, Types of Data in Cluster Analysis, Partitioning Methods, Hierarchical Methods, Density Based Methods, Grid Based Methods, Model Based Clustering Methods, Clustering High Dimensional Data - Predictive Analytics – Data analysis using R.

UNIT IV MINING DATA STREAMS 7

Streams: Concepts – Stream Data Model and Architecture - Sampling data in a stream - Mining Data Streams and Mining Time-series data - Real Time Analytics Platform (RTAP) Applications - Case Studies - Real Time Sentiment Analysis, Stock Market Predictions.

UNIT V BIG DATA FRAMEWORKS 9

Introduction to NoSQL – Aggregate Data Models – Hbase: Data Model and Implementations – Hbase Clients – Examples – .Cassandra: Data Model – Examples – Cassandra Clients – Hadoop Integration. Pig – Grunt – Pig Data Model – Pig Latin – developing and testing Pig Latin scripts. Hive – Data Types and File Formats – HiveQL Data Definition – HiveQL Data Manipulation – HiveQL Queries.

TOTAL: 45 PERIODS

OUTCOMES:

At the end of this course, the students will be able to:

- Understand how to leverage the insights from big data analytics
- Analyze data by utilizing various statistical and data mining approaches
- Perform analytics on real-time streaming data
- Understand the various NoSql alternative database models

REFERENCES:

1. Bill Franks, “Taming the Big Data Tidal Wave: Finding Opportunities in Huge Data Streams with Advanced Analytics”, Wiley and SAS Business Series, 2012.
2. David Loshin, "Big Data Analytics: From Strategic Planning to Enterprise Integration with Tools, Techniques, NoSQL, and Graph", 2013.
3. Learning R – A Step-by-step Function Guide to Data Analysis, Richard Cotton, O’Reilly Media, 2013.
4. Michael Berthold, David J. Hand, “Intelligent Data Analysis”, Springer, Second Edition, 2007.
5. Michael Minelli, Michelle Chambers, and Ambiga Dhiraj, "Big Data, Big Analytics: Emerging Business Intelligence and Analytic Trends for Today's Businesses", Wiley, 2013.
6. P. J. Sadalage and M. Fowler, "NoSQL Distilled: A Brief Guide to the Emerging World of Polyglot Persistence", Addison-Wesley Professional, 2012.

BC5010 WIRELESS SECURITY

L	T	P	C
3	0	0	3

OBJECTIVES:

- To understand the fundamentals of wireless security.
- To understand the security issues in bluetooth and Wi-Fi.
- To explore the security issues in WiMAX and mobile telecommunication networks.
- To understand the security issues in ad-hoc and wireless sensor networks.
- To study the hacking techniques in IEEE 802.11.

UNIT I WIRELESS SECURITY FUNDAMENTALS 9

Vulnerabilities of Wired and Wireless Networks-Security in the digital age-Threats and risks to telecommunications systems- Vulnerabilities from wirelines to wireless communications-Fundamental Security Mechanisms-Basics on security-Secure communication protocols and VP Nimplementation-Authentication-Access control.

UNIT II SECURITY IN BLUETOOTH AND WI-FI 9

Bluetooth security- Security mode in Bluetooth-Authentication and pairing- Bluetooth encoding-Attacks- Wi-Fi Security- Attacks on wireless networks- Security in the IEEE 802.11 standard- Security in 802.1x- Security in 802.11i.

UNIT III SECURITY IN WIMAX AND MOBILE TELECOMMUNICATION NETWORKS 9

WiMAX low layers- Security in 802.16-2004- Security in IEEE-802.16e standard- Telecommunication Security- Signaling- Security in the GSM- GPRS security- 3G security.

UNIT IV SECURITY IN AD HOC AND WIRELESS SENSOR NETWORKS 9

Attacks to routing protocols- Security mechanisms- Auto-configuration-Authentication issue within ad hoc networks- Group key management within ad hoc networks-Attacks on wireless sensor networks and counter measures- Prevention mechanisms: authentication and traffic protection.

UNIT V HACKING 802.11 WIRELESS TECHNOLOGY 9

Introduction to 802.11 Hacking- Scanning and Enumerating 802.11 Networks- Attacking 802.11 Wireless Networks- Attacking WPA-Protected 802.11 Networks- Attack 802.11 Wireless Clients.

TOTAL : 45 PERIODS

OUTCOMES :

On completing this course, the student will be able to:

- Identify various possibilities for security threats in wireless networks.
- Handle the security threats in Bluetooth and Wi-Fi networks.
- Solve the security attacks in WiMAX and mobile telecommunication networks.
- Prevent the attacks in ad-hoc and wireless sensor networks.
- Protect the 802.11 Networks from attacks.

REFERENCES:

1. Alan Holt , Chi-Yu Huang, "802.11 Wireless Networks- Security and Analysis", Springer, 2010.
2. Hakima Chaouchi, Maryline Laurent-Maknavicius, "Wireless and Mobile Network Security-Security Basics, Security in On-the-shelf and Emerging Technologies", John Wiley & Sons Inc, 2009.
3. Johnny Cache, Joshua Wright, Vincent Liu, "Hacking Exposed Wireless: Wireless Security Secrets & Solutions", Second Edition, McGraw-Hill, 2010.
4. Lei Chen, Jiahuang Ji, Zihong Zhang, "Wireless Network Security: Theories and Applications", Higher Education Press, 2013.

BC5011	ETHICAL HACKING AND NETWORK DEFENSE	L	T	P	C
		3	0	0	3

OBJECTIVES:

To understand and analyse Information security threats & coutermeasures
To perform security auditing & testing
To understand issues relating to ethical hacking
To study & employ network defense measures
To understand penetration and security testing issues

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 of the hackers,Tools used for the reconnaissance phase.Port Scanning - Introduction, using port scanning tools, ping sweeps, Scripting Enumeration-Introduction, Enumerating windows OS & Linux OS

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 Networks.

TOTAL : 45 PERIODS

OUTCOMES:

Upon successful completion of this course, a student will be able to:

- understand vulnerabilities, mechanisms to identify vulnerabilities/threats/attacks
- perform penetration & security testing
- become a professional ethical hacker

REFERENCES:

1. Kimberly Graves, "Certified Ethical Hacker", Wiley India Pvt Ltd, 2010
2. Michael T. Simpson, "Hands-on Ethical Hacking & Network Defense", Course Technology, 2010
3. Rajat Khare, "Network Seuciryt and Ethical Hacking", Luniver Press, 2006
4. Ramachandran V, BackTrack 5 Wireless Penetration Testing Beginner's Guide (3rd ed.). Packt Publishing, 2011
5. Thomas Mathew, "Ethical Hacking", OSB publishers, 2003