ANNA UNIVERSITY, CHENNAI
NON - AUTONOMOUS COLLEGES AFFILIATED ANNA UNIVERSITY
M.E. BIOMETRICS AND CYBER SECURITY

REGULATIONS – 2021
CHOICE BASED CREDIT SYSTEM

1. PROGRAMME EDUCATIONAL OBJECTIVES(PEOs):

I. Systematically plan, implement, and monitor cyber security mechanisms to ensure end-to-end security of IT assets and thus strengthen the cyber ecosystem.
II. Possess the technical knowledge and skills needed to protect and defend computer systems and networks from cyber threats and attacks.
III. Effectively identify, analyze, and remediate cyber attacks, through sustainable research-based biometric solutions for enterprises.
IV. Adopt ethical practices, collaborate with team members and team leaders, and engage in constant updation of technical knowledge.
V. Strongly focus on ingenious ideas and critical analysis to serve the society, locally and internationally as entrepreneurs in the field of cyber security.

2. PROGRAMME OUTCOMES

1 An ability to independently carry out research/investigation and development work to solve practical problems
2 An ability to write and present a substantial technical report/document
3 Students should be able to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program
4 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.
5 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.
6 Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

ANNA UNIVERSITY, CHENNAI
NON - AUTONOMOUS COLLEGES AFFILIATED ANNA UNIVERSITY
M.E. BIOMETRICS AND CYBER SECURITY
REGULATIONS – 2021
CHOICE BASED CREDIT SYSTEM
I TO IV SEMESTERS CURRICULA AND SYLLABI
SEMESTER I

S. NO.	COURSE CODE	COURSE TITLE	CATE-GORY	PERIODS PER WEEK			TOTAL CONTACT PERIODS	CREDITS
				L	T	P		
THEORY								
1.	MA4113	Algebra and Probability	FC	3	1	0	4	4
2.	RM4151	Research Methodology and IPR	RMC	2	0	0	2	2
3.	CP4151	Advanced Data Structures and Algorithms	PCC	3	0	0	3	3
4.	BC4151	Biometric Systems	PCC	3	0	2	5	4
5.	CE4151	Principles of Cyber Security	PCC	3	0	2	5	4
6.	BC4152	Cyber Forensics and Investigation	PCC	3	0	0	3	3
7.		Audit Course – I*	AC	2	0	0	2	0
PRACTICALS								
8.	CP4161	Advanced Data Structures and Algorithms Laboratory	PCC	0	0	4	4	2
			TOTAL	**19**	**1**	**8**	**28**	**22**

*Audit course is optional

SEMESTER II

S. NO.	COURSE CODE	COURSE TITLE	CATE-GORY	PERIODS PER WEEK			TOTAL CONTACT PERIODS	CREDITS
				L	T	P		
THEORY								
1.	BC4201	Applied Cryptography	PCC	3	0	2	5	4
2.	CP4252	Machine Learning	PCC	3	0	2	5	4
3.	BC4202	Biometric Data Processing	PCC	3	0	0	3	3
4.	BC4291	Ethical Hacking	PCC	3	0	2	5	4
5.		Professional Elective I	PEC	3	0	0	3	3
6.		Audit Course – II*	AC	2	0	0	2	0
PRACTICALS								
7.	BC4211	Biometric Data Processing Laboratory	PCC	0	0	4	4	2
8.	BC4212	Term Paper Writing and Seminar	EEC	0	0	2	2	1
			TOTAL	**17**	**0**	**12**	**29**	**21**

*Audit course is optional

SEMESTER III

S. NO.	COURSE CODE	COURSE TITLE	CATE-GORY	PERIODS PER WEEK			TOTAL CONTACT PERIODS	CREDITS
				L	T	P		
THEORY								
1.		Professional Elective II	PEC	3	0	0	3	3
2.		Professional Elective III	PEC	3	0	0	3	3
3.		Professional Elective IV	PEC	3	0	2	5	4
4.		Open Elective	OEC	3	0	0	3	3
PRACTICALS								
5.	BC4311	Project Work I	EEC	0	0	12	12	6
			TOTAL	**12**	**0**	**14**	**26**	**19**

SEMESTER IV

S. NO.	COURSE CODE	COURSE TITLE	CATE-GORY	PERIODS PER WEEK			TOTAL CONTACT PERIODS	CREDITS
				L	T	P		
PRACTICALS								
1.	BC4411	Project Work II	EEC	0	0	24	24	12
			TOTAL	**0**	**0**	**24**	**24**	**12**

TOTAL NO. OF CREDITS: 74

PROFESSIONAL ELECTIVES
SEMESTER II, ELECTIVE I

S. NO.	COURSE CODE	COURSE TITLE	CATE-GORY	PERIODS PER WEEK			TOTAL CONTACT PERIODS	CREDITS
				L	T	P		
1.	BC4001	Principles of Secure Coding	PEC	3	0	0	3	3
2.	NE4251	Network Security	PEC	3	0	0	3	3
3.	BC4002	Public Key Infrastructure	PEC	3	0	0	3	3
4.	BC4003	Operating Systems Security	PEC	3	0	0	3	3
5.	CP4391	Security Practices	PEC	3	0	0	3	3
6.	MU4252	Media Security	PEC	3	0	0	3	3

SEMESTER III, ELECTIVE II

S. NO.	COURSE CODE	COURSE TITLE	CATE-GORY	PERIODS PER WEEK			TOTAL CONTACT PERIODS	CREDITS
				L	T	P		
1.	BC4004	Biometric Security	PEC	3	0	0	3	3
2.	BC4005	Secure Systems Engineering	PEC	3	0	0	3	3
3.	BC4006	Cloud Security	PEC	3	0	0	3	3
4.	BC4007	Firewall and VPN Security	PEC	3	0	0	3	3
5.	BC4008	Mobile and Digital Forensics	PEC	3	0	0	3	3

SEMESTER III, ELECTIVE III

S. NO.	COURSE CODE	COURSE TITLE	CATE-GORY	PERIODS PER WEEK			TOTAL CONTACT PERIODS	CREDITS
				L	T	P		
1.	BC4009	Access Control and Identity Management Systems	PEC	3	0	0	3	3
2.	IF4095	Social Network Analysis	PEC	3	0	0	3	3
3.	BC4010	Data Privacy	PEC	3	0	0	3	3
4.	BC4011	Security in Cyber-Physical Systems	PEC	3	0	0	3	3
5.	BC4012	Cryptanalysis	PEC	3	0	0	3	3
6.	BC4013	Data Analytics for Fraud Detection	PEC	3	0	0	3	3

SEMESTER III, ELECTIVE IV

S. NO.	COURSE CODE	COURSE TITLE	CATE-GORY	PERIODS PER WEEK			TOTAL CONTACT PERIODS	CREDITS
				L	T	P		
1.	CP4291	Internet of Things	PEC	3	0	2	5	4
2.	BC4014	Malware Analysis	PEC	3	0	2	5	4
3.	BC4015	Secure Software Design and Development	PEC	3	0	2	5	4
4.	BC4016	Security Assessment and Risk Analysis	PEC	3	0	2	5	4
5.	BC4017	Steganography and Digital Watermarking	PEC	3	0	2	5	4
6.	CP4072	Blockchain Technologies	PEC	3	0	2	5	4
7.	BC4018	Web Security	PEC	3	0	2	5	4

AUDIT COURSES (AC)

Registration for any of these courses is optional to students

SL. NO	COURSE CODE	COURSE TITLE	PERIODS PER WEEK			CREDITS
			L	T	P	
1.	AX4091	English for Research Paper Writing	2	0	0	0
2.	AX4092	Disaster Management	2	0	0	0
3.	AX4093	Constitution of India	2	0	0	0
4.	AX4094	நற்றமிழ் இலக்கியம்	2	0	0	0

FOUNDATION COURSES (FC)

S. NO	COURSE CODE	COURSE TITLE	PERIODS PER WEEK			CREDITS	SEMESTER
			Lecture	Tutorial	Practical		
1.	MA4113	Algebra and Probability	3	1	0	4	I

PROFESSIONAL CORE COURSES (PCC)

S. NO	COURSE CODE	COURSE TITLE	PERIODS PER WEEK			CREDITS	SEMESTER
			Lecture	Tutorial	Practical		
1.	CP4151	Advanced Data Structures and Algorithms	3	0	0	3	I
2.	BC4151	Biometric Systems	3	0	2	4	I
3.	CE4151	Principles of Cyber Security	3	0	2	4	I
4.	BC4152	Cyber Forensics and Investigation	3	0	0	3	I
5.	CP4161	Advanced Data Structures and Algorithms Laboratory	0	0	4	2	I
6.	BC4201	Applied Cryptography	3	0	2	4	II
7.	CP4252	Machine Learning	3	0	2	4	II
8.	BC4202	Biometric Data Processing	3	0	0	3	II
9.	BC4291	Ethical Hacking	3	0	2	4	II
10.	BC4211	Biometric Data Processing Laboratory	0	0	4	2	II

RESEARCH METHODOLOGY AND IPR COURSES (RMC)

S. NO	COURSE CODE	COURSE TITLE	PERIODS PER WEEK			CREDITS	SEMESTER
			Lecture	Tutorial	Practical		
1.	RM4151	Research Methodology and IPR	2	0	0	2	1

EMPLOYABILITY ENHANCEMENT COURSES (EEC)

S. NO	COURSE CODE	COURSE TITLE	PERIODS PER WEEK			CREDITS	SEMESTER
			Lecture	Tutorial	Practical		
1.	BC4212	Term Paper Writing and Seminar	0	0	2	1	II
2.	BC4311	Project Work I	0	0	12	6	III
3.	BC4411	Project Work II	0	0	24	12	IV

SUMMARY

Sl. No.	NAME OF THE PROGRAMME: M.E. BIOMETRICS AND CYBER SECURITY						
	SUBJECT AREA	CREDITS PER SEMESTER				CREDITS TOTAL	
		I	II	III	IV		
1.	FC	04	00	00	00	04	
2.	PCC	16	17	00	00	33	
3.	PEC	00	03	10	00	13	
4.	RMC	02	00	00	00	02	
5.	OEC	00	00	03	00	03	
6.	EEC	00	01	06	12	19	
7.	Non Credit/Audit Course	✓	✓	00	00		
8.	**TOTAL CREDIT**	**22**	**21**	**19**	**12**	**74**	

MA4113 **ALGEBRA AND PROBABILITY** **L T P C**
3 1 0 4

COURSE OBJECTIVES:

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

UNIT I RANDOM VARIABLES 12

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

UNIT II RANDOM PROCESSES 12

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

UNIT III TESTING OF HYPOTHESIS 12

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

UNIT IV GROUPS AND RINGS 12

Groups: Definition – Properties – Homomorphism - Isomorphism – Cyclic groups – Cosets – Lagrange's theorem. Rings: Definition – Sub rings – Integral domain – Field – Integer modulo n – Ring homomorphism.

UNIT V FINITE FIELDS AND POLYNOMIALS 12

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

TOTAL : 60 PERIODS

COURSE OUTCOMES:

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

- analyze the performance in terms of probabilities and distributions achieved by the determined solutions.
- classify various random processes and solve problems involving stochastic processes.
- apply the basic principles underlying statistical inference (estimation and hypothesis testing).
- apply the basic notions of groups, rings, fields which will then be used to solve related problems.
- explain the fundamental concepts of advanced algebra and their role in modern mathematics and applied contexts.

REFERENCES:

1. Devore J.L.," Probability and Statistics for Engineering and sciences", Cengage learning, 9th Edition, Boston,2017.
2. Grimaldi R. P. and Ramana B.V., "Discrete and Combinatorial Mathematics", Pearson Education, 5th Edition, New Delhi, 2007.
3. Johnson R. A. and Gupta C.B., "Miller and Freund's Probability and Statistics for Engineers", Pearson India Education, Asia, 9th Edition, New Delhi, 2017.
4. Ibe. O.C., " Fundamentals of Applied Probability and Random Processes", Elsevier U.P., 1st Indian Reprint, 2007.

RM4151 RESEARCH METHODOLOGY AND IPR L T P C
2 0 0 2

UNIT I RESEARCH DESIGN 6

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

UNIT II DATA COLLECTION AND SOURCES 6

Measurements, Measurement Scales, Questionnaires and Instruments, Sampling and methods. Data - Preparing, Exploring, examining and displaying.

UNIT III DATA ANALYSIS AND REPORTING 6

Overview of Multivariate analysis, Hypotheses testing and Measures of Association.
Presenting Insights and findings using written reports and oral presentation.

UNIT IV INTELLECTUAL PROPERTY RIGHTS 6

Intellectual Property – The concept of IPR, Evolution and development of concept of IPR, IPR development process, Trade secrets, utility Models, IPR & Biodiversity, Role of WIPO and WTO in IPR establishments, Right of Property, Common rules of IPR practices, Types and Features of IPR Agreement, Trademark, Functions of UNESCO in IPR maintenance.

UNIT V PATENTS 6

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

TOTAL : 30 PERIODS

REFERENCES

1. Cooper Donald R, Schindler Pamela S and Sharma JK, "Business Research Methods", Tata McGraw Hill Education, 11e (2012).
2. Catherine J. Holland, "Intellectual property: Patents, Trademarks, Copyrights, Trade Secrets", Entrepreneur Press, 2007.
3. David Hunt, Long Nguyen, Matthew Rodgers, "Patent searching: tools & techniques", Wiley, 2007.
4. The Institute of Company Secretaries of India, Statutory body under an Act of parliament, "Professional Programme Intellectual Property Rights, Law and practice", September 2013.

CP4151 ADVANCED DATA STRUCTURES AND ALGORITHMS L T P C
3 0 0 3

COURSE 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 & COMPLEXITY ANALYSIS 9

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

UNIT II HIERARCHICAL DATA STRUCTURES 9

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

UNIT III GRAPHS 9

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

UNIT IV ALGORITHM DESIGN TECHNIQUES 9

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

UNIT V NP COMPLETE AND NP HARD 9

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

TOTAL : 45 PERIODS

SUGGESTED ACTIVITIES:

1. Write an algorithm for Towers of Hanoi problem using recursion and analyze the complexity (No of disc-4)
2. Write any one real time application of hierarchical data structure
3. Write a program to implement Make_Set, Find_Set and Union functions for Disjoint Set Data Structure for a given undirected graph G(V,E) using the linked list representation with simple implementation of Union operation
4. Find the minimum cost to reach last cell of the matrix from its first cell
5. Discuss about any NP completeness problem

COURSE OUTCOMES:

CO1: Design data structures and algorithms to solve computing problems.

CO2: Choose and implement efficient data structures and apply them to solve problems.

CO3: Design algorithms using graph structure and various string-matching algorithms to solve real-life problems.

CO4: Design one's own algorithm for an unknown problem.

CO5: Apply suitable design strategy for problem solving.

REFERENCES:

1. S.Sridhar," Design and Analysis of Algorithms", Oxford University Press, 1st Edition, 2014.
2. Adam Drozdex, "Data Structures and algorithms in C++", Cengage Learning, 4th Edition, 2013.
3. T.H. Cormen, C.E.Leiserson, R.L. Rivest and C.Stein, "Introduction to Algorithms", Prentice Hall of India, 3rd Edition, 2012.
4. Mark Allen Weiss, "Data Structures and Algorithms in C++", Pearson Education, 3rd Edition, 2009.
5. E. Horowitz, S. Sahni and S. Rajasekaran, "Fundamentals of Computer Algorithms", University Press, 2nd Edition, 2008.
6. Alfred V. Aho, John E. Hopcroft, Jeffrey D. Ullman, "Data Structures and Algorithms", Pearson Education, Reprint 2006.

BC4151 BIOMETRIC SYSTEMS L T P C

3 0 2 4

COURSE OBJECTIVES:

- To learn and understand biometric technologies and their functionalities.
- To learn the role of biometric in the organization
- To Learn the computational methods involved in the biometric systems.
- To expose the context of Biometric Applications
- To learn to develop applications with biometric security

UNIT I INTRODUCTION 9+6

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

UNIT II FINGERPRINT, FACE AND IRIS AS BIOMETRICS 9+6

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

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

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

UNIT III PRIVACY ENHANCEMENT AND MULTIMODAL BIOMETRICS 9+6

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

UNIT IV WATERMARKING TECHNIQUES & BIOMETRICS: SCOPE AND FUTURE 9+6

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

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

UNIT V IMAGE ENHANCEMENT TECHNIQUES & BIOMETRICS STANDARDS 9+6

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

LIST OF EXPERIMENTS (Experiments can be designed with similar use cases as below):

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

COURSE OUTCOMES:

CO1: Identify the various biometric technologies.
CO2: Design of biometric recognition for the organization.
CO3: Develop simple applications for privacy.
CO4: Understand the need of biometric in the society
CO5: Understand the research in biometric techniques.

TOTAL : 75 PERIODS

REFERENCES:

1. G R Sinha and Sandeep B. Patil, Biometrics: Concepts and Applications, Wiley, 2013
2. Paul Reid, Biometrics for Network Security, Pearson Education, 2003
3. Samir Nanavathi, Micheal Thieme, Raj Nanavathi, Biometrics – Identity verification in a networked world, Wiley – dream Tech, 2002.
4. John D Woodward, Jr.; Nicholas M Orlans; Peter T Higgins, Biometrics – The Ultimate Reference, Wiley Dreamtech.College Publications, 2015.
5. Khalid Saeed, “New Directions in Behavioral Biometrics', CRC Press 2020.
6. Ruud M. Bolle, Sharath Pankanti, Nalini K. Ratha, Andrew W. Senior, Jonathan H. Connell, Guide to Biometrics, Springer 2009.
7. Rafael C. Gonzalez, Richard Eugene Woods, Digital Image Processing using MATLAB, 2nd Edition, Tata McGraw-Hill Education 2010.

CE4151 PRINCIPLES OF CYBER SECURITY L T P C
3 0 2 4

COURSE OBJECTIVES:

- To know the cyber security principles, as well as the issues, policy and standards
- To understand the difference between threat, risk, attack and vulnerability and how threats materialize into attacks .
- To be familiar with the typical threats, attacks and exploits and the motivations behind them.
- To study the defensive techniques against these attacks
- To describe remedies for various existing cyber security breaches and to show the methodologies required to make future systems less prone to security failures

UNIT I INTRODUCTION TO CYBER SECURITY 9

Basic Cyber Security Concepts, layers of security, Vulnerability, Threat, Harmful acts, Internet Governance - Controls - Authentication -Access Control and Cryptography – Challenges and Constraints, Computer Criminals, CIA Triad, Motive of Attackers, Active Attacks, Passive Attacks, Software Attacks, Hardware Attacks, Spectrum of Attacks, Browser Attacks - Web Attacks Targeting Users - Obtaining User or Website Data - Email Attacks, Taxonomy of various attacks, IP spoofing, Methods of defence, Security Models, risk management, Cyber Threats-Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage, Malicious code , Countermeasures.

UNIT II SECURITY IN OPERATING SYSTEMS & 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. Cloud Security Tools & Techniques,

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

Comprehensive Cyber Security Policy 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 HomeLand Security.

TOTAL:45 PERIODS

LIST OF EXPERIMENTS:

1. Implementation to gather information from any PC connected to the LAN using whois, port scanners, network scanning, Angry IP scanners etc.
2. Implementation of Claiming ownership of digital entity
3. Implementation of Tracing the digital theft in cyberspace
4. Implementation of Data hiding in different image types
5. Implementation of MITM- attack using wireshark/ network sniffers
6. Implementation of Windows security using firewall and other tools
7. Implementation to identify web vulnerabilities, using OWASP project
8. Implementation of IT Audit, malware analysis and Vulnerability assessment and generate the report.
9. Implementation of OS hardening and RAM dump analysis to collect the artifacts and other information.
10. Implementation of Cyber Forensics tools for Disk Imaging, Data acquisition, Data extraction and Data Analysis and recovery.

TOTAL: 30 PERIODS

TOTAL:45+30=75 PERIODS

COURSE OUTCOMES:

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

CO1: Understand the broad set of technical, social & political aspects of Cyber Security

CO2: Describe the operational and organizational Cyber Security Aspects

CO3: Identify and assess different types of Cyber security breaches and possible solutions for a robust system

CO4: understand cyber-attacks, and also how to protect the entire Internet community from such attacks

CO5: Demonstrate the ability to select and design among available security solutions based on different domains of cyber systems

REFERENCES:

1. Charles P. Pfleeger Shari Lawrence Pfleeger Jonathan Margulies, Security in Computing, 5th Edition , Pearson Education , 2018
2. Nina Godbole, Sunit Belapure, “Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives”, Wiley India Pvt. Ltd. , 2011
3. B. B. Gupta, D. P. Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithms, Applications, and Perspectives, CRC Press, 2018.
4. George K.Kostopoulos, Cyber Space and Cyber Security, CRC Press, 2013.
5. Martti Lehto, Pekka Neittaanmäki, Cyber Security: Analytics, Technology and Automation, Springer International Publishing Switzerland 2015
6. Chwan-Hwa (John) Wu, J. David Irwin, Introduction to Computer Networks and Cyber security, CRC Press T&F Group, 2013.
7. James Graham, Richard Howard and Ryan Otson, Cyber Security Essentials, CRC Press T&F Group, 2011

BC4152 CYBER FORENSICS AND INVESTIGATION L T P C
3 0 0 3

COURSE OBJECTIVES:

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

UNIT I CYBER FORENSICS SCIENCE 9

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

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

UNIT II NETWORK SECURITY FORENSICS SYSTEM AND SERVICES 9

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

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

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

UNIT III DIGITAL FORENSICS PRESERVATION AND FORENSIC DATA ANALYSIS 9

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

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

UNIT IV CLOUD, NETWORK AND MOBILE FORENSICS 9

Working with the cloud vendor, obtaining evidence, reviewing logs and APIs

Mobile Forensics techniques, Mobile Forensics Tools - Android Device – Analysis- Android Malware – iOS Forensic Analysis – SIM Forensic Analysis – Case study

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

UNIT V LEGAL ASPECTS OF DIGITAL FORENSICS 9

IT Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT IPC and CrPC , Electronic Communication Privacy ACT, Legal Policies, Act 2000, amendment of IT Act 2008.

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

TOTAL : 45 PERIODS

COURSE OUTCOMES:

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

CO1: Understand the responsibilities and liabilities of a computer forensic investigator

CO2: Identify potential sources of electronic evidence.

CO3: Understand the importance of maintaining the integrity of digital evidence.

CO4: Demonstrate the ability to perform basic forensic data acquisition and analysis using computer and network based applications and utilities.

CO5: Understand relevant legislation and codes of ethics.

REFERENCES:

1. J. R. Vacca, Computer forensics: Computer Crime Scene investigation, 2nd Ed. Hanover, NH, United States: Charles River Media, 2002, Laxmi Publications, 1st Edition, 2015.
2. C. Altheide, H. Carvey, and R. Davidson, Digital Forensics with Open Source Tools: Using Open Source Platform Tools for Performing Computer Forensics on Target Systems: Windows, Mac, Linux, Unix, etc, 1st Ed. United States: Syngress, 2011.
3. S. Bommisetty, R. Tamma, and H. Mahalik, Practical Mobile Forensics: Dive into Mobile Forensics on IOS, Android, Windows, and blackBerry devices with this action-packed, practical guide. United Kingdom: Packt Publishing, 2014.
4. G. Gogolin, Digital Forensics Explained, 1st Ed. Boca Raton, FL: CRC Taylor & Francis, 1st Edition, Auerbach Publications, 2013.
5. A. Hoog and J. McCash, Android forensics: Investigation, Analysis, and Mobile Security for Google Android. Waltham, MA: Syngress Media, U.S., 2011.
6. B. Nelson, A. Phillips, F. Enfinger, and C. Steuart, Guide to Computer Forensics and Investigations, Second edition, 2nd Ed. Boston: Thomson Course Technology, 2009.
7. C. Altheide and H. Carvey, “Digital Forensics with Open Source Tools”, 2011 Publisher(s): Syngress.
8. J. Sammons, “The Basics of Digital Forensics- The Primer for Getting Started in Digital Forensics”, 1st Edition, Syngress, 2012.
9. Nelson, Phillips and Enfinger Steuart, “Guide to Computer Forensics and Investigations”, 6th Edition, Cengage Learning, New Delhi, 2020.

CP4161	ADVANCED DATA STRUCTURES AND ALGORITHMS LABORATORY	L T P C 0 0 4 2

COURSE 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
- To understand the problems such as matrix chain multiplication, activity selection and Huffman coding
- To understand the necessary mathematical abstraction to solve problems.

LIST OF EXPERIMENTS:

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

HARDWARE/SOFTWARE REQUIREMENTS

1: 64-bit Open source Linux or its derivative
2: Open Source C++ Programming tool like G++/GCC

TOTAL : 60 PERIODS

COURSE OUTCOMES:

CO1: Design and implement basic and advanced data structures extensively
CO2: Design algorithms using graph structures
CO3: Design and develop efficient algorithms with minimum complexity using design techniques
CO4: Develop programs using various algorithms.
CO5: Choose appropriate data structures and algorithms, understand the ADT/libraries, and use it to design algorithms for a specific problem.

REFERENCES:

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

BC4201 APPLIED CRYPTOGRAPHY L T P C
3 0 2 4

COURSE OBJECTIVES:

- To understand OSI security architecture and classical encryption techniques.
- To 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 MATHEMATICAL FOUNDATION AND NUMBER THEORY 10

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

UNIT II BLOCK CIPHERS AND MODES OF OPERATIONS 8

Simplified DES - Data Encryption Standard-Block cipher principles-block cipher modes of 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 SIGNATURE 9

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

UNIT V APPLICATIONS OF CRYPTOGRAPHIC ALGORITHMS 10

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

TOTAL:45 PERIODS

PRACTICALS:

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

TOTAL:30 PERIODS

COURSE OUTCOMES:

CO1: Compare various Cryptographic Techniques
CO2: Understand security issues, practices and principles in various applications
CO3: Learn to analyse the security of the in-built cryptosystems
CO4: Develop cryptographic algorithms for information security
CO5: Develop authentication schemes for identity and membership authorization

TOTAL: 75 PERIODS

REFERENCES

1. Bruce Schneier and Neils Ferguson, “Practical Cryptography”, First Edition, Wiley Dreamtech India Pvt Ltd, 2003.
2. J. H. Silverman, A Friendly Introduction to Number Theory, 4th Ed. Boston: Pearson, 2019 (ISBN No.: 978 9353433079, 935343307X
3. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security : Private Communications in a Public World”, Prentice Hall of India, Second Edition, 2016. (UNIT V)
4. Douglas R Stinson and Maura B. Paterson, “Cryptography – Theory and practice”, Fourth Edition, CRC Press,2018 (UNIT -I)
5. William Stallings, Cryptography and Network Security, Seventh Edition, Pearson Education, 2017. (UNIT I,II,III,IV)

CP4252 **MACHINE LEARNING** **L T P C**
3 0 2 4

COURSE OBJECTIVES:

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

UNIT I INTRODUCTION AND MATHEMATICAL FOUNDATIONS 9

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

UNIT II SUPERVISED LEARNING 9

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

UNIT III UNSUPERVISED LEARNING AND REINFORCEMENT LEARNING 9

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

UNIT IV PROBABILISTIC METHODS FOR LEARNING- 9

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

UNIT V NEURAL NETWORKS AND DEEP LEARNING 9

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

45 PERIODS

SUGGESTED ACTIVITIES:

1. Give an example from our daily life for each type of machine learning problem
2. Study at least 3 Tools available for Machine Learning and discuss pros & cons of each
3. Take an example of a classification problem. Draw different decision trees for the example and explain the pros and cons of each decision variable at each level of the tree
4. Outline 10 machine learning applications in healthcare
5. Give 5 examples where sequential models are suitable.
6. Give at least 5 recent applications of CNN

PRACTICAL EXERCISES: 30 PERIODS

1. Implement a Linear Regression with a Real Dataset (https://www.kaggle.com/harrywang/housing). Experiment with different features in building a model. Tune the model's hyperparameters.

2. Implement a binary classification model. That is, answers a binary question such as "Are houses in this neighborhood above a certain price?"(use data from exercise 1). Modify the classification threshold and determine how that modification influences the model. Experiment with different classification metrics to determine your model's effectiveness.

3. Classification with Nearest Neighbours. In this question, you will use the scikit-learn's KNN classifer to classify real vs. fake news headlines. The aim of this question is for you to read the scikit-learn API and get comfortable with training/validation splits. Use California Housing Dataset

4. In this exercise, you'll experiment with validation sets and test sets using the dataset. Split a training set into a smaller training set and a validation set. Analyze deltas between training set and validation set results. Test the trained model with a test set to determine whether your trained model is overfitting. Detect and fix a common training problem.

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

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

7. Project - (in Pairs) Your project must implement one or more machine learning algorithms and apply them to some data.

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

List of Projects (datasets available)

1. Sentiment Analysis of Product Reviews
2. Stock Prediction

3. Sales Forecasting
4. Music Recommendation
5. Handwriting Digit Classification
6. Fake News Detection
7. Sports Prediction
8. Object Detection
9. Disease Prediction

COURSE OUTCOMES:

Upon the completion of course, students will be able to

CO1: Understand and outline problems for each type of machine learning

CO2: Design a Decision tree and Random forest for an application

CO3: Implement Probabilistic Discriminative and Generative algorithms for an application and analyze the results.

CO4: Use a tool to implement typical Clustering algorithms for different types of applications.

CO5: Design and implement an HMM for a Sequence Model type of application and identify applications suitable for different types of Machine Learning with suitable justification.

TOTAL:75 PERIODS

REFERENCES

1. Stephen Marsland, "Machine Learning: An Algorithmic Perspective", Chapman & Hall/CRC, 2nd Edition, 2014.
2. Kevin Murphy, "Machine Learning: A Probabilistic Perspective", MIT Press, 2012
3. Ethem Alpaydin, "Introduction to Machine Learning", Third Edition, Adaptive Computation and Machine Learning Series, MIT Press, 2014
4. Tom M Mitchell, "Machine Learning", McGraw Hill Education, 2013.
5. Peter Flach, "Machine Learning: The Art and Science of Algorithms that Make Sense of Data", First Edition, Cambridge University Press, 2012.
6. Shai Shalev-Shwartz and Shai Ben-David, "Understanding Machine Learning: From Theory to Algorithms", Cambridge University Press, 2015
7. Christopher Bishop, "Pattern Recognition and Machine Learning", Springer, 2007.
8. Hal Daumé III, "A Course in Machine Learning", 2017 (freely available online)
9. Trevor Hastie, Robert Tibshirani, Jerome Friedman, "The Elements of Statistical Learning", Springer, 2009 (freely available online)
10. Aurélien Géron , Hands-On Machine Learning with Scikit-Learn and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems 2nd Edition, o'reilly, (2017)

BC4202	BIOMETRIC DATA PROCESSING	L	T	P	C
		3	0	0	3

COURSE OBJECTIVES:

- To understand the basics of Biometric Data processing
- To model and visualize the transformation of image
- To understand the evolution of object detection
- To learn the computational methods involved in the biometric systems

UNIT I INTRODUCTION TO BIOMETRIC DATA PROCESSING 9

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

UNIT II IMAGE PROCESSING FUNDAMENTALS AND OPERATIONS OF BIOMETRIC SYSTEM 10

Image processing and Basic image operations: - pattern recognition/statistics, Error types. image, acquisition, type, point operations, Geometric transformations. Linear interpolation, brightness correction, histogram, Convolution, linear/non-linear filtering, Guassian, Median, Min, gray level reduction. Special filters, enhancement filter, Laplacian, unsharp masking, high boost filtering, sharpening special filtering, Edge detection, DFT , inverse of DFT.

Operations of a biometric system - verification and identification, performance of a biometric system, FAR, FRR, GAR, ERR, DET and ROC curve, Failure to Acquire (FTA), Failure to Enroll (FTE), applications of biometrics, characteristics.

UNIT III OBJECT DETECTION AND FACE RECOGNITION 9

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

Face Recognition – Eigenfaces (PCA), Linear Discriminant Analysis (LDA) and Fisherfaces, Independent Component Analysis (ICA), Neural Networks (NN) and Support Vector Machines (SVM), Kernel Methods, Face biometric database

UNIT IV FINGERPRINT AND IRIS RECOGNITION 9

Fingerprint recognition – Sensing, feature extraction, Enhancement and binarization, Minutiae extraction, matching – correlation based methods, minutiae based methods, ridge feature based methods, performance evaluation, synthetic fingerprint generation

IRIS recognition system, Active Contours, Flexible Generalized Embedded Coordinates, Fourier-based Trigonometry and Correction for Off-Axis Gaze, Detecting and excluding eyelashes by Statistical Inference, Alternative Score Normalization Rules

UNIT V 3D BIOMETRIC and BIOMETRIC DATA APPLICATIONS 8

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

COURSE OUTCOMES:

CO1: Explain the principles and types of biometric data processing
CO2: Use Image processing operations for biometrics
CO3: Apply techniques required for object detection and face recognition
CO4: Develop techniques required for fingerprint and iris recognition
CO5: Design and evaluate biometric applications

TOTAL: 45 PERIODS

REFERENCES

1. Ruud M. Bolle, SharathPankanti, Nalini K. Ratha, Andrew W. Senior, Jonathan H. Connell, “Guide to Biometrics",Springer 2013 (Unit 1)
2. Rafael C. Gonzalez, Richard Eugene Woods, "Digital Image Processing using MATLAB", 2nd Edition, Tata McGraw-Hill Education 2010 (Unit 2)
3. Claus Vielhauer, "Biometric user authentication for IT security: from fundamentals to handwriting", Vol. 18. Springer Science & Business Media, 2005 (Unit 2)
4. Anil Jain, Patrick Flynn, and Arun A. Ross, eds. "Handbook of biometrics", Springer Science & Business Media, 2007 (Unit 3 & 4)
5. Richard O. Duda, David G.Stork, Peter E. Hart, "Pattern Classification", Wiley 2007
6. Julian Ashbourn, "Biometrics in the New World”, Springer 2014.
7. Zhang, David, Lu, Guangming,“3D Biometrics Systems and Applications”, Springer 2013. (Unit 5)

BC4291 ETHICAL HACKING L T P C
3 0 2 4

COURSE OBJECTIVES:

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

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 Network

TOTAL:45 PERIODS

LIST OF EXPERIMENTS:

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

TOTAL:30 PERIODS

COURSE OUTCOMES:

CO1: Understand vulnerabilities, mechanisms to identify vulnerabilities/threats/attacks
CO2: Use tools to identify vulnerable entry points
CO3: Identify vulnerabilities using sniffers at different layers
CO4: Handle web application vulnerabilities
CO5: Identify attacks in wireless networks

TOTAL:75 PERIODS

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. RajatKhare, "Network Security 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
6. Matthew Hickey, Jennifer Arcuri, "Hands on Hacking: Become an Expert at Next Gen Penetration Testing and Purple Teaming", 1st Edition, Wiley, 2020.
7. Jon Ericson, Hacking: The Art of Exploitation, 2nd Edition, NoStarch Press, 2008.

BC4211 BIOMETRIC DATA PROCESSING LABORATORY L T P C
0 0 4 2

COURSE OBJECTIVES:

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

LIST OF EXPERIMENTS:

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

COURSE OUTCOMES:

CO1:Design and Apply Image Enhancement and Segmentation.
CO2:Design and Apply Fingerprint Acquisition and Feature Extraction
CO3: Design and Apply Face and Iris Acquisition and Feature Extraction
CO4:Design and Apply 3D Biometric
CO5: Implement Mobile Biometrics

TOTAL: 60 PERIODS

BC4212 TERM PAPER WRITING AND SEMINAR L T P C
0 0 2 1

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

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

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

Activities to be carried out

Activity	Instructions	Submission week	Evaluation
Selection of area of interest and Topic Stating an Objective	You are requested to select an area of interest, topic and state an objective	2nd week	**3 %** Based on clarity of thought, current relevance and clarity in writing
Collecting Information about your area & topic	1. List 1 Special Interest Groups or professional society 2. List 2 journals 3. List 2 conferences, symposia or workshops 4. List 1 thesis title 5. List 3 web presences (mailing lists, forums, news sites) 6. List 3 authors who publish regularly in your area 7. Attach a call for papers (CFP) from your area.	3rd week	**3%** (the selected information must be area specific and of international and national standard)
Collection of Journal papers in the topic in the context of the objective – collect 20 & then filter	• You have to provide a complete list of references you will be using- Based on your objective -Search various digital libraries and Google Scholar • When picking papers to read - try to: • Pick papers that are related to each other in some ways and/or that are in the same field so that you can write a meaningful survey out of them, • Favour papers from well-known journals and conferences, • Favour "first" or "foundational" papers in the field (as indicated in other people's survey paper), • Favour more recent papers, • Pick a recent survey of the field so you can quickly gain an overview, • Find relationships with respect to each other and to your topic area (classification scheme/categorization) • Mark in the hard copy of papers whether complete work or section/sections of the paper are being considered	4th week	**6%** (the list of standard papers and reason for selection)

Reading and notes for first 5 papers	Reading Paper Process • For each paper form a Table answering the following questions: • What is the main topic of the article? • What was/were the main issue(s) the author said they want to discuss? • Why did the author claim it was important? • How does the work build on other's work, in the author's opinion? • What simplifying assumptions does the author claim to be making? • What did the author do? • How did the author claim they were going to evaluate their work and compare it to others? • What did the author say were the limitations of their research? • What did the author say were the important directions for future research? Conclude with limitations/issues not addressed by the paper (from the perspective of your survey)	5th week	**8%** (the table given should indicate your understanding of the paper and the evaluation is based on your conclusions about each paper)
Reading and notes for next5 papers	Repeat Reading Paper Process	6th week	**8%** (the table given should indicate your understanding of the paper and the evaluation is based on your conclusions about each paper)
Reading and notes for final 5 papers	Repeat Reading Paper Process	7th week	**8%** (the table given should indicate your understanding of the paper and the evaluation is based on your conclusions about each paper)
Draft outline 1 and Linking papers	Prepare a draft Outline, your survey goals, along with a classification / categorization diagram	8th week	**8%** (this component will be evaluated based on the linking and classification among the papers)
Abstract	Prepare a draft abstract and give a presentation	9th week	**6%**

			(Clarity, purpose and conclusion) **6%** Presentation & Viva Voce
Introduction Background	Write an introduction and background sections	10th week	**5%** (clarity)
Sections of the paper	Write the sections of your paper based on the classification / categorization diagram in keeping with the goals of your survey	11thweek	**10%** (this component will be evaluated based on the linking and classification among the papers)
Your conclusions	Write your conclusions and future work	12th week	**5%** (conclusions – clarity and your ideas)
Final Draft	Complete the final draft of your paper	13th week	**10%** (formatting, English, Clarity and linking) **4%** Plagiarism Check Report
Seminar	A brief 15 slides on your paper	14th & 15th week	**10%** (based on presentation and Viva-voce)

TOTAL: 30 PERIODS

BC4001 PRINCIPLES OF SECURE CODING L T P C
3 0 0 3

COURSE OBJECTIVES:

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

UNIT I SOFTWARE SECURITY 8

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

UNIT II STATIC ANALYSIS 7

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

UNIT III STRINGS AND INTEGER SECURITY 10

Strings: Common String manipulating Errors, String Vulnerabilities and Exploits, Mitigation Strategies for strings, String handling functions, Runtime protecting strategies, Dynamic Memory

Management: Memory Management errors in C and C++ , Notable Vulnerabilities. Integer Security: Integer data Type, Integer Conversions, Integer Operations, Integer Vulnerabilities, Mitigation Strategies.

UNIT IV HANDLING INPUTS AND EXCEPTIONS 10

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

UNIT V SECURE WEB APPLICATIONS 10

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

COURSE OUTCOMES:

CO1: Apply secure coding practices when developing a software.
CO2: Understand and perform a static analysis and security review of a software code.
CO3: Evaluate strings and integer vulnerabilities in a software code.
CO4: Handle inputs, overflow mechanisms, errors and exceptions in a software code.
CO5: Design a secure web application by performing input and output validation techniques on the web.

TOTAL: 45 PERIODS

REFERENCES

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

NE4251 NETWORK SECURITY L T P C
3 0 0 3

COURSE OBJECTIVES:

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

UNIT I INTRODUCTION TO NETWORK SECURITY 9

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

UNIT II SYMMETRIC AND ASYMMETRIC CIPHERS 9

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

UNIT III SECURITY ISSUES IN INTERNET PROTOCOL 9

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

UNIT IV SECURITY IN OTHER LAYERS 9

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

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

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

COURSE OUTCOMES:

CO1: To design cryptographic algorithms and carry out their implementation.
CO2: To carry out cryptanalysis on cipher.
CO3: To be able to design and implement security based internet protocols.
CO4: To carry out system security for other layers.
CO5: To understand the importance of intrusion detection and prevention system and wireless hacking.

TOTAL: 45 PERIODS

REFERENCES

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

BC4002 **PUBLIC KEY INFRASTRUCTURE** **L T P C**
3 0 0 3

COURSE OBJECTIVES:

- Understand public key infrastructure technology
- Understand Public Key Algorithms
- Understand centralized and decentralized infrastructure
- Understand concept of digital certificates
- Learn various security threats to E-commerce

UNIT I OVERVIEW OF PKI TECHNOLOGY 9

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

UNIT II PKI ALGORITHMS 9

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

UNIT III DESIGN, IMPLEMENTATION, MANAGEMENT 9

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

UNIT IV E-COMMERCE SECURITY THREATS 9

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

UNIT V APPLICATIONS OF PKI 9

Applications of PKI: Trust Models, Deployment and Operation, X.509 Certificates, E-commerce: the building blocks – Trusted Business Environment for E-commerce, Certification, Certification Practice and Policy, Registration, Certification usage and revocation, PKI in Electronic Government; Trusted Services and PKI: Technology Commonality in Approaches and Government Initiatives.

COURSE OUTCOMES:

After the completion of this course, students will be able to

CO1: Understand the core fundamentals of public key infrastructures
CO2: Develop and use secure Public Key Algorithms
CO3: Design, Implement and Manage the public key infrastructures
CO4: Identify the security threats to E-commerce
CO5: Evaluate use of PKI for different applications

TOTAL: 45 PERIODS

REFERENCES

1. Larry Caffrey, Rogers W'O. Okot-Uma, "Trusted Services and Public Key Infrastructure PKI) International Council of Information Technology in Government Administration, 2000.
2. Cartisle Adams, Steve Lloyd, "Understanding PKI: Concepts, Standards and Deployment Considerations:, Pearson Education, 2003.
3. Vacca R Vacca, "Public Key Infrastructure: Building Trusted Applications and Web Services", CRC Press LLC 2004.
4. Andrew Nash, William Daune, Celia Joseph and Derek Brink, "PKI – Implementing and Managing E-Security, Tata McGraw-Hill Edition, 2001.
5. GrayP.Schneider, "Electronic Commerce", Fourth Annual Edition, 2003.
6. Roberta Bragg, Mark Phodes-Ousley and Keith Strassberg, "The Complete Reference Network Security", Tata McGraw-Hill Edition, 2004.
7. Bruce Schneier, "Applied Cryptography", John Willey and Sons, 2001.

BC4003 OPERATING SYSTEM SECURITY L T P C
3 0 0 3

COURSE OBJECTIVES:

- To learn the basics of operating system concepts and its security mechanisms.
- To understand the protection threats to an operating system and various protection mechanisms.
- To understand the security goals and protect the operating system from threats and attacks.
- To learn the security concepts for a server and analyze the various networking technologies for the Linux operating system.

UNIT I INTRODUCTION 9

Introduction, Computer system organization and architecture, Operating system structure and operations, Process Management, Memory Management, file systems management Protection and security, Scheduling Algorithms, Interprocess Communication

UNIT II OPERATING SYSTEMS PROTECTION 9

Protection Goals, Protection Threats, Access Control Matrix, Access Control Lists(ACL's), Capability Lists(C-lists), Protection systems, Lampson's access matrix, mandatory protection systems, Reference monitor, Secure operating system definition

UNIT III OPERATING SYSTEM SECURITY 9

Security Goals, Security Threats, Security Attacks- Trojan Horses, Viruses and Worms, Buffer Overflow attacks and Techniques, Formal Aspects of Security, Encryption- Attacks on Cryptographic Systems, Encryption Techniques, Authentication and Password Security, Intrusion detection, malware defenses, UNIX and Windows Security

UNIT IV SYSTEM ADMINISTRATION 9

Security Basics, Securing the Server Itself, Maintenance and Recovery, Monitoring and Audit, Introduction to Linux Systems, Configuration Management, Log Auditing and Vulnerability Assessment.

UNIT V LINUX NETWORKING 9

Networking Technologies: DHCP, DNS, NFS/ISCSI, SMTP, SNMP, LAMP, Firewall/IDS/SSH, Securing Linux. Case Studies: Security and Protection- MULTICS, UNIX, LINUX and Windows, Windows and Linux Coexisting.

COURSE OUTCOMES:

CO1: Understand the operating system's security concepts and its security control mechanisms.

CO2:Demonstrate the Access control matrix, access control list and Lampson's access matrix

CO3: Identify the Encryption Techniques, Authentication and Password Security issues

CO4: Understand the security threats and attacks on cryptographic systems

CO5: Apply the security and protection mechanisms for different operating systems

TOTAL: 45 PERIODS

REFERENCES

1. Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, "Operating System Concepts", 10th Edition, Wiley Publication, 2018 (Unit 1)
2. Dhananjay M. Dhamdhere, "Operating Systems: A Concept-Based Approach", 3rd Edition, McGraw- Hill, 2015 (Unit 2, 3)
3. Jordan Krause, "Windows Server 2016 Security, Certificates, and Remote Access Cookbook: Recipe-based guide for security, networking and PKI in Windows Server 2016", Pckt Publishing, 2018.
4. Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley, Dan Mackin,"Linux Administration Handbook", Fifth Edition, Addison-Wesley, 2017 (Unit 5)
5. Promod Chandra P Bhat,, "An Introduction to Operating Systems: Concepts and practice", 5th Edition, Prentice Hall of India, 2019.
6. William Stalling, "Operating System: Internals and Design Principles", 9th Edition, Pearson, 2017.
7. Tom Adelstein and Bill Lubanovic, "Linux System Administration", 1st Edition, Shroff., 2012.

CP4391 SECURITY PRACTICES L T P C
3 0 0 3

COURSE OBJECTIVES:

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

UNIT I SYSTEM SECURITY 9

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

UNIT II NETWORK SECURITY 9

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

UNIT III SECURITY MANAGEMENT 9

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

UNIT IV CYBER SECURITY AND CLOUD SECURITY 9

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

UNIT V PRIVACY AND STORAGE SECURITY 9

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

COURSE OUTCOMES:

CO1: Understand the core fundamentals of system security
CO2: Apply the security concepts to wired and wireless networks
CO3: Implement and Manage the security essentials in IT Sector
CO4: Explain the concepts of Cyber Security and Cyber forensics
CO5: Be aware of Privacy and Storage security Issues.

TOTAL: 45 PERIODS

REFERENCES

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

MU4252 **MEDIA SECURITY** **L T P C**
3 0 0 3

COURSE OBJECTIVES:

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

UNIT I CRYPTANALYSIS AND DIGITAL RIGHTS MANAGEMENT 9

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

Suggested Activities:

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

Suggested Evaluation Methods:

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

UNIT II DIGITAL WATERMARKING BASICS 9

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

Suggested Activities:

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

Suggested Evaluation Methods:

1. Assignment on ECC.
2. Tutorial on DRM products.

UNIT III DIGITAL WATERMARKING SCHEMES AND PROTOCOLS 9

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

Suggested Activities:

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

Suggested Evaluation Methods:

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

UNIT IV STEGANOGRAPHY AND STEGANALYSIS 9

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

Suggested Activities:

1. An application to be developed using Steganography.

Suggested Evaluation Methods:

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

UNIT V MULTIMEDIA ENCRYPTION 9

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

Suggested Activities:

1. Case study on forensic data.
2. Case study on forgery detection.

Suggested Evaluation Methods:

1. Group discussion on case studies.

COURSE OUTCOMES:

CO1: Identify the security challenges and issues that may arise in any system.
CO2: Implement the concepts of steganography, digital watermarking techniques.
CO3: Design secure applications using steganography and watermarking schemes
CO4: Apply concepts on digital rights management while developing secure systems
CO5: Design a secure multimedia system using encryption and privacy preservation techniques.

TOTAL: 45 PERIODS

REFERENCES

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

BC4004 **BIOMETRIC SECURITY** **L T P C**
3 0 0 3

COURSE OBJECTIVES:

- To understand the various attacks in biometric systems.
- To acquire knowledge on biometric authentication protocols
- To understand the various key distribution and management strategies.
- To understand how to deploy encryption techniques to secure data using biometric
- To gain knowledge on security criteria and adopt security measures for a biometric system

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 MULTIMODAL 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.

COURSE OUTCOMES:

CO1: Implement basic security algorithms required by the biometric system

CO2: Analyze the vulnerabilities in biometric system and hence be able to design a security Solution

CO3: Analyze the possible security attacks in complex real time systems and their effective Countermeasures

CO4: Identify the security issues in the network and resolve it

CO5: Formulate research problems in the biometric security field

TOTAL: 45 PERIODS

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

BC4005 SECURE SYSTEMS ENGINEERING L T P C
3 0 0 3

COURSE OBJECTIVES:

- Study of designing secure systems.
- Understandthe micro architectural level of security.
- Understand hardware, operating system, and application layer vulnerabilities.
- Study countermeasures for system level attacks.

UNIT I HARDWARE SECURITY 8

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

UNIT II MICRO ARCHITECTURAL SECURITY 7

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

UNIT III OPERATING SYSTEM SECURITY 10

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

UNIT IV APPLICATION SECURITY 10

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

UNIT V SYSTEMS SECURITY 10

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

COURSE OUTCOMES:

CO1: Identify and analyse vulnerabilities at hardware level
CO2: Identify micro architectural level security
CO3: Analyse and apply countermeasures to operating system level attacks
CO4: Apply malware analysis techniques at system level
CO5: Understand and analyse application level security

TOTAL: 45 PERIODS

REFERENCES

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

BC4006	CLOUD SECURITY	L	T	P	C
		3	0	0	3

COURSE OBJECTIVES:

- To Introduce Cloud Computing terminology, definition & concepts
- To understand the security design and architectural considerations for Cloud
- To understand the Identity, Access control in Cloud
- To follow best practices for Cloud security using various design patterns
- To be able to monitor and audit cloud applications for security

UNIT I FUNDAMENTALS OF CLOUD COMPUTING 9

Understand what is Cloud computing, Architectural and Technological Influences of Cloud Computing, Understand the Cloud deployment models, Public, Private, Community and Hybrid models, Scope of Control, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Cloud Computing Roles, Risks and Security Concerns

UNIT II SECURITY DESIGN AND ARCHITECTURE FOR CLOUD 9

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

UNIT III ACCESS CONTROL AND IDENTITY MANAGEMENT 10

Understand the access control requirements for Cloud infrastructure, Enforcing Access Control Strategies, Authentication and Authorization, Roles-based Access Control, Multi-factor authentication, Host, storage and network access control options, OS Hardening and minimization, securing remote access, Verified and measured boot, Firewalls, Intruder Detection, Intruder prevention and honeypots, User Identification, Authentication, and Authorization in Cloud

Infrastructure, Identity & Access Management, Single Sign-on, Identity Federation, Identity providers and service consumers, The role of Identity provisioning

UNIT IV CLOUD SECURITY DESIGN PATTERNS 9

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

UNIT V MONITORING, AUDITING AND MANAGEMENT 8

Proactive activity monitoring, Incident Response, Monitoring for unauthorized access, malicious traffic, abuse of system privileges, intrusion detection, events and alerts, Auditing – Record generation, Reporting and Management, Tamper-proofing audit logs, Quality of Services, Secure Management, User management, Identity management, Security Information and Event Management

COURSE OUTCOMES:

CO1: Understand the cloud concepts and fundamentals.
CO2: Explain the security challenges in cloud.
CO3: Define cloud policy and Identity and Access Managements.
CO4: Understand various risks, and audit and monitoring mechanisms in cloud.
CO5: Define the various architectural and design considerations for security in cloud.

TOTAL PERIODS:45

REFERENCES

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

BC4007 FIREWALL AND VPN SECURITY L T P C

3 0 0 3

COURSE OBJECTIVES:

- Identify and assess current and anticipated security risks and vulnerabilities
- Develop a network security plan and policies
- Establish a VPN to allow IPSec remote access traffic
- Monitor, evaluate and test security conditions and environment
- Develop critical situation contingency plans and disaster recovery plan
- Implement/test contingency and backup plans and coordinate with stakeholders
- Monitor, report and resolve security problems

UNIT I INTRODUCTION 9

Introduction, Types of Firewalls, Ingress and Egress Filtering, Types of Filtering, Network Address Translation (NAT), Application Proxy, Circuit Proxy, Content Filtering, Software versus Hardware

Firewalls, IPv4 versus IPv6 Firewalls, Dual-Homed and Triple-Homed Firewalls, Placement of Firewalls.

UNIT II VPN FUNDAMENTALS 9

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

UNIT III EXPLORING THE DEPTHS OF FIREWALLS 9

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

UNIT IV OVERVIEW OF INDUSTRIAL CONTROL SYSTEMS 9

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

UNIT V SCADA PROTOCOLS 9

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

COURSE OUTCOMES:

After the completion of this course, student will be able to

CO1: Show the fundamental knowledge of Firewalls and it types

CO2: Construct a VPN to allow Remote Access, Hashing, connections with Cryptography and VPN Authorization

CO3: Elaborate the knowledge of depths of Firewalls, Interpreting firewall logs, alerts, Intrusion and Detection

CO4: Explain the design of Control Systems of SCAD, DCS, PLC‘s and ICS‘s

CO5: Evaluate the SCADA protocols like RTU, TCP/IP, DNP3, OPC,DA/HAD

TOTAL: 45 PERIODS

REFERENCES

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

BC4008 **MOBILE AND DIGITAL FORENSICS** **L T P C**
3 0 0 3

COURSE OBJECTIVES:

- Understand the basics of wireless technologies and security.
- Become knowledgeable in mobile phone forensics and android forensics.
- Learn the methods of investigation using digital forensic techniques.

UNIT I INTRODUCTION **9**

Overview of wireless technologies and security: Personal Area Networks, Wireless Local Area Networks, Metropolitan Area Networks, Wide Area Networks. Wireless threats, vulnerabilities and security: Wireless LANs, War Driving, WarChalking, War Flying, Common Wi-fi security recommendations, PDA Security, Cell Phones and Security, Wireless DoS attacks, GPS Jamming, Identity theft.

UNIT II CONFIDENTIALITY, INTEGRITY, AVAILABILITY TRIAD IN MOBILE **9**

Confidentiality, integrity, availability (CIA) triad in mobile phones-Voice, SMS and Identification data interception in GSM: Introduction, practical setup and tools, implementation- Software and Hardware Mobile phone tricks: Netmonitor, GSM network service codes, mobile phone codes, catalog tricks and AT command set- SMS security issues

UNIT III MOBILE PHONE FORENSICS **12**

Mobile phone forensics: crime and mobile phones, evidences, forensic procedures, files present in SIM card, device data, external memory dump, evidences in memory card, operators systems- Android forensics: Procedures for handling an android device, imaging android USB mass storage devices, logical and physical techniques

UNIT IV DIGITAL FORENSICS **7**

Digital forensics: Introduction – Evidential potential of digital devices: closed vs. open systems, evaluating digital evidence potential- Device handling: seizure issues, device identification, networked devices and contamination

UNIT V DIGITAL FORENSICS EXAMINATION PRINCIPLES **8**

Digital forensics examination principles: Previewing, imaging, continuity, hashing and evidence locations- Seven element security model- developmental model of digital systems- audit and logs- Evidence interpretation: Data content and context

COURSE OUTCOMES:

After the completion of this course, student will be able to

CO1: Undertand the basics of mobile and digital security.
CO2: Explain mobile phone forensics and android forensics.
CO3: Analyse issues in Digital forensics.
CO4: Understand the common data privacy techniques.
CO5: Examine and analyze Digital forensics techniques.

TOTAL: 45 PERIODS

REFERENCES

1. Gregory Kipper, “Wireless Crime and Forensic Investigation”, Auerbach Publications, 2007

2. Iosif I. Androulidakis, “Mobile phone security and forensics: A practical approach”, Springer publications, Second Edition, 2016
3. Andrew Hoog, “Android Forensics: Investigation, Analysis and Mobile Security for Google Android”, Elsevier publications, 2011
4. Angus M.Marshall, “ Digital forensics: Digital evidence in criminal investigation”, John – Wiley and Sons, 2008

BC4009 ACCESS CONTROL AND IDENTITY MANAGEMENT SYSTEMS L T P C
3 0 0 3

COURSE OBJECTIVES:

- To understand the importance of Identity Access and Management (IAM),
- To understand the regulations and industry standards for Identity management
- To build the capability to assess the risks, understand the techniques for Identity and authentication
- To learn and devise various access control techniques and 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- DiscretionaryAccess Controls (DAC), Non Discretionary Access Controls (NAC), Mandatory Access Controls (MAC), Role-Based Access Controls (RBAC), Task Based Access Controls (TBAC),Lattice-Based Access Controls. Access Control Methodologies and Implementations - Access Control Administration - Account Administration - Account, Log, and Journal Monitoring/Audits- Access Rights and Permissions**.**

UNIT IV ACCESS CONTROL SYSTEMS 9

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

UNIT V CASE STUDIES 9

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

COURSE OUTCOMES:

After the completion of this course, student will be able to

CO1: Understand the role of IAM with emerging mobile information society, compliance and regulations and industry standards for Identity management.

CO2: Perform risks assessment

CO3: Compare various access control techniques.

CO4: Choose the appropriate Programming Models and approach

CO5: Carry out analysis and report strength and weakness if IAM in a given typical online applications.

TOTAL: 45 PERIODS

REFERENCES

1. MessaoudBenantar, "Access Control Systems: Security, Identity Management and Trust Models", IBM Corp, Austin, TX, USA. Library of Congress, ISBN-13: 978-0-387-00445-7 e-ISBN-13: 978-0-387-27716-5.
2. Masha Garibyan, Simon McLeish and John Paschoud, "Access and Identity Management for Libraries: Controlling access to online information", Facet Publishing 2014 www.facetpublishing.co.uk.
3. Frank Bresz, Ernst & Young LLP et. al., "Identity and Access Management GTAG", The Institute of Internal Auditors, Altamonte Springs, FL32701-4201. 2007.
4. Ray Wagner, "Identity and Access Management", Digital 2020, ISSA Journal , June 2014 , www.issa.org.
5. Dan Sullivan, "The Definitive Guide to Security Management", Realtimepublishers.com chapter5:Identity and Access Management http://www3.ca.com/ebook/.
6. Elena Ferrari and M. Tamer A-zsu , "Access Control In Data Management Systems", Morgan & Claypool Publishers, 2010.

IF4095 **SOCIAL NETWORK ANALYSIS** **L T P C**
3 0 0 3

COURSE OBJECTIVES:

- Formalise different types of entities and relationships as nodes and edges and represent this information as relational data.
- Understand the fundamental concepts in analyzing the large-scale data that are derived from social networks
- Understand the basic concepts and principles of different theoretical models of social networks analysis.

- Transform data for analysis using graph-based and statistics-based social network measures
- Choose among social network designs based on research goals

UNIT I GRAPH THEORY AND STRUCTURE 10

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

UNIT II SOCIAL NETWORK GRAPH ANALYSIS 9

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

UNIT III INFORMATION DIFFUSION IN SOCIAL NETWORKS 9

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

UNIT IV CASCADING IN SOCIAL NETWORKS 8

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

UNIT V LINK ANALYSIS & COMMUNITY DETECTION 9

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

SUGGESTED ACTIVITIES:

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

COURSE OUTCOMES:

CO1: Plan and execute network analytical computations.
CO2: Implement mining algorithms for social networks
CO3: Analyze and evaluate social communities.
CO4: Use social network analysis in behavior analytics

CO5: Perform mining on large social networks and illustrate the results.

TOTAL: 45 PERIODS

REFERENCES

1. Practical Social Network Analysis with Python, Krishna Raj P. M. Ankith Mohan and K. G. Srinivasa. Springer, 2018
2. SOCIAL NETWORK ANALYSIS: METHODS AND APPLICATIONS, STANLEY WASSERMAN, and KATHERINE F' AUST. CAMBRIDGE UNIVERSITY PRESS, 2012
3. Social Network Analysis: History, Theory and Methodology by Christina Prell, SAGE Publications, 1st edition, 2011
4. Sentiment Analysis in Social Networks, Federico Alberto Pozzi, Elisabetta Fersini, Enza Messina, and Bing. LiuElsevier Inc, 1st edition, 2016
5. Social Network Analysis, John Scott. SAGE Publications, 2012

BC4010 **DATA PRIVACY** **L T P C**
3 0 0 3

COURSE OBJECTIVES:

- To understand the basics of data privacy
- To create architectural, algorithmic and technological foundations for the maintenance of the privacy
- To become knowledgeable in Static Data Anonymization Methods.
- To analyse anonymization algorithms
- To understand the concept of privacy preservation

UNIT I INTRODUCTION **9**

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

UNIT II STATIC DATA ANONYMIZATION ON MULTIDIMENSIONAL DATA **9**

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

UNIT III STATIC DATA ANONYMIZATION ON COMPLEX DATA STRUCTURES **9**

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

UNIT IV STATIC DATA ANONYMIZATION ON THREATS TO ANONYMIZED DATA **9**

Static Data Anonymization on Threats to Anonymized Data, Threats to Data Structures, Threats by Anonymization Techniques, Randomization, k-Anonymization, l-Diversity, t-Closeness. Dynamic

Data Protection: Tokenization, Understanding Tokenization, Use Cases for Dynamic Data Protection, Benefits of Tokenization Compared to Other Methods, Components for Tokenization

UNIT V PRIVACY PRESERVING 9

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

COURSE OUTCOMES:

CO1: Become familiar with the basics of privacy.
CO2: Understand how privacy is formalized.
CO3: Understand the common data privacy techniques.
CO4: Able to analyse Static Data Anonymization
CO5: Understand and analyse privacy preservation techniques

TOTAL: 45 PERIODS

REFERENCES

1. N. Venkataramanan and A. Shriram, "Data privacy: Principles and practice". CRC Press, 2016. ISBN: 978-1-49-872104-2
2. A. Hundepool, J. Domingo-Ferrer, L. Franconi, S. Giessing, and E. S. Nordholt, P.D. Wolf, “Statistical disclosure control”, Wiley, John & Sons, 2012. ISBN No.: 978-1-11-997815-2
3. G. T. Duncan, M. Elliot, J.-J. Salazar-González, J.-J. Salazar-Gonzalez, and J. J. Salazar, "Statistical confidentiality: Principles and practice", Springer-Verlag New York, 2011. ISBN: 978-1-44-197801-1
4. C. C. Aggarwal and P. S. Yu, "Privacy-preserving data mining: Models and Algorithms", Springer-Verlag New York, 2008. (ISBN No.: 978-0-387-70992-5)

BC4011 SECURITY IN CYBER-PHYSICAL SYSTEMS L T P C
3 0 0 3

COURSE OBJECTIVES:

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

UNIT I INTRODUCTION TO CYBER-PHYSICAL SYSTEMS 6

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

UNIT II CPS - PLATFORM COMPONENTS 10

CPS - Platform components: CPS HW platforms - Processors, Sensors, Actuators, CPS Network - WirelessHart, CAN, Automotive Ethernet, CPS Sw stack – RTOS, Scheduling Real Time control

tasks Principles of Automated Control Design: Dynamical Systems and Stability Controller Design Techniques, Stability Analysis: CLFs, MLFs, stability under slow switching, Performance under Packet drop and Noise

UNIT III USING MATLAB 8

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

UNIT IV CPS SAFETY ASSURANCE AND SOFTWARE ANALYSIS 12

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

UNIT V CPS SECURITY 8

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

COURSE OUTCOMES:

After the completion of this course, student will be able to

CO1: Understand the core principles behind CPS.
CO2: Identify safety specifications and critical properties.
CO3: Understand abstraction in system designs.
CO4: Express pre and postconditions and invariants for CPS models.
CO5: Identify CPS security threats and do the software analysis.

TOTAL: 45 PERIODS

REFERENCES

1. Raj Rajkumar, Dionisio De Niz , and Mark Klein, Cyber-Physical Systems, Addison-Wesley Professional
2. Rajeev Alur, Principles of Cyber-Physical Systems, MIT Press, 2015.
3. André Platzer, Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics., Springer, 2010. 426 pages,ISBN 978-3-642-14508-7.
4. Jean J. Labrosse, Embedded Systems Building Blocks: Complete and Ready-To-Use Modules in C, The publisher, Paul Temme, 2011.
5. Jean-Paul A. Yaacoub, Ola Salman, Hassan N. Noura, NesrineKaaniche, Ali Chehab, Mohamad Malli, "Cyber-physical systems security: Limitations, issues and future trends", Microprocessors and Microsystems, Vol 77, 2020, ISSN 0141-9331 (Unit 5)
6. Sajal Das, Krishna Kant, and Nan Zhang, “Handbook on Securing Cyber-Physical CriticalInfrastructure – Foundations & Challenges”, Morgan Kaufmann, 2012.
7. Awad, A.I., Furnell, S., Paprzycki, M., Sharma, S.K., Security in Cyber-Physical Systems Foundations and Applications,Springer International Publishing, 2021

BC4012 **CRYPTANALYSIS** **L T P C**
3 0 0 3

COURSE OBJECTIVES:

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

UNIT I INTRODUCTION 9

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

UNIT II TRANSPOSITION 9

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

UNIT III BRUTE FORCE CRYPTANALYSIS 9

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

UNIT IV ALGORITHMS FOR FUNCTIONS 9

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

UNIT V LATTICE BASED CRYPTANALYSIS 9

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

COURSE OUTCOMES:

After the completion of this course, student will be able to

CO1: Apply cryptanalysis in system design to protect it from various attacks.

CO2: Identify and investigate vulnerabilities and security threats and the mechanisms to counter them.

CO3: Analyze security of cryptographic algorithm against brute force attacks, birthday attacks.

CO4: Design cryptographic algorithms for functions and carry out their implementation.

CO5: Understand the importance lattice based cryptanalysis

TOTAL: 45 PERIODS

REFERENCES

1. Elementary Cryptanalysis A Mathematical Approach by Abraham Sinkov, The mathematical Association of America (Inc).
2. Algorithmic Cryptanalysis, by Antoine joux, 1st Edition, CRC Press, 2009.
3. Algebraic Cryptanalysis, Bard Gregory, Springer, 2009
4. Cryptanalysis of Number Theoretic Ciphers, Sameul S. Wag staff, Chapman & Hall/CRC, 2002.
5. Cryptanalysis: A Study of Cipher and Their Solution, Helen F. Gaines,1989

BC4013 DATA ANALYTICS FOR FRAUD DETECTION L T P C

3 0 0 3

COURSE OBJECTIVES:

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

UNIT I INTRODUCTION 9

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

UNIT II DATA ANALYSIS CYCLE 9

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

UNIT III DATA ANALYTICAL TESTS 9

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

UNIT IV ADVANCED DATA ANALYTICAL TESTS 9

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

UNIT V ELECTRONIC PAYMENTS FRAUD PREVENTION 9

Payroll Fraud, Expense Reimbursement Schemes, Register disbursement schemes

COURSE OUTCOMES:

CO1:Formulate reasons for using data analysis to detect fraud.
CO2: Explain characteristics and components of the data and assess its completeness.
CO3:Identify known fraud symptoms and use digital analysis to identify unknown fraud symptoms.
CO4:Automate the detection process.
CO5:Verify results and understand how to prosecute fraud

TOTAL: 45 PERIODS

REFERENCES

1. Sunder Gee, “Fraud and Fraud Detection: A Data Analytics Approach”, Wiley, 2014, ISBN: 978-1-118-77965-1
2. Bart Baesens, Veronique Van Vlasselaer, WouterVerbeke, "Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection", Wiley and SAS Business Series, 2015
3. Han, Kamber, “Data Mining Concepts and Techniques”, 3rd Ed., Morgan Kaufmann Publishers, 2012
4. Jure Leskovec, Anand Rajaraman, Jeffrey David Ullman, “Mining of Massive Datasets”, Cambridge University Press, 2nd Ed., 2014.

CP4291	INTERNET OF THINGS	L	T	P	C
		3	0	2	4

COURSE OBJECTIVES:

- To Understand the Architectural Overview of IoT
- To Understand the IoT Reference Architecture and Real World Design Constraints
- To Understand the various IoT levels
- To understand the basics of cloud architecture
- To gain experience in Raspberry PI and experiment simple IoT application on it

UNIT I INTRODUCTION **9+6**

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

UNIT II IoT ARCHITECTURE, GENERATIONS AND PROTOCOLS **9+6**

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

UNIT III IoT PROTOCOLS AND TECHNOLOGY **9+6**

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

UNIT IV CLOUD ARCHITECTURE BASICS **9+6**

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

UNIT V IOT PROJECTS ON RASPBERRY PI **9+6**

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

SUGGESTED ACTIVITIES:

1. Develop an application for LED Blink and Pattern using Arduino or Raspberry Pi
2. Develop an application for LED Pattern with Push Button Control using Arduino or Raspberry Pi
3. Develop an application for LM35 Temperature Sensor to display temperature values using arduino or Raspberry Pi
4. Develop an application for Forest fire detection end node using Raspberry Pi device and sensor
5. Develop an application for home intrusion detection web application
6. Develop an application for Smart parking application using python and Django for web application

COURSE OUTCOMES:

CO1: Understand the various concept of the IoT and their technologies
CO2: Develop the IoT application using different hardware platforms
CO3: Implement the various IoT Protocols
CO4: Understand the basic principles of cloud computing
CO5: Develop and deploy the IoT application into cloud environment

TOTAL: 75 PERIODS

REFERENCES:

1. Arshdeep Bahga, Vijay Madisetti, Internet of Things: A hands-on approach, Universities Press, 2015
2. Dieter Uckelmann, Mark Harrison, Florian Michahelles (Eds), Architecting the Internet of Things, Springer, 2011
3. Peter Waher, 'Learning Internet of Things', Packt Publishing, 2015
4. Ovidiu Vermesan Peter Friess, 'Internet of Things – From Research and Innovation to Market Deployment', River Publishers, 2014
5. N. Ida, Sensors, Actuators and Their Interfaces: A Multidisciplinary Introduction, 2nd EditionScitech Publishers, 202014
6. Reese, G. (2009). Cloud Application Architectures: Building Applications and Infrastructure in the Cloud. Sebastopol, CA: O'Reilly Media, Inc. (2009)

BC4014 MALWARE ANALYSIS **L T P C**
3 0 2 4

COURSE OBJECTIVES:

- To introduce the fundamentals of malware, types and its effects
- To enable to identify and analyse various malware types by static analysis
- To enable to identify and analyse various malware types by dynamic analysis

- To deal with detection, analysis, understanding, controlling, and eradication of malware

UNIT I INTRODUCTIONAND BASIC ANALYSIS 9

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

UNIT II ADVANCED STATIC ANALYSIS 9

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

UNIT III ADVANCED DYNAMIC ANALYSIS 9

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

UNIT IV MALWARE FUNCTIONALITY 9

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

UNIT V ANDROID MALWARE ANALYSIS 9

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

TOTAL: 45 PERIODS

PRACTICALS:

1. Experimentation on Initial Infection Vectors and Malware Discovery
2. Implementation on Sandboxing Malware and Gathering Information From Runtime Analysis
3. Implementation on Portable Executable (PE32) File Format
4. Implementation on Executable Metadata and Executable Packers
5. Experimentation on Malware Self - Defense, Compression, and Obfuscation Techniques
6. Experimentation on Malware behaviour analysis
7. Experimentation on analyzing Malicious Microsoft Office and Adobe PDF Documents
8. Experimentation on Mobile malware analysis
9. Experimentation on Packing and Unpacking of malware
10. Experimentation on Rootkit AntiForensics and Covert Channels
11. Experimentation on Modern Rootkit Analysis
12. Experimentation on Malware traffic analysis

Implement of real time applications for the following malware analysis

1. Static analysis of malwares
2. Dynamic analysis of malwares.
3. Classification of malwares based on their behaviour.
4. Usage of tools to classify malware
5. Advanced malware analysis
6. Android malware analysis
7. Applying antivirus tools in various applications
8. Malware report documentation

TOTAL: 30 PERIODS
TOTAL: 45+30=75 PERIODS

COURSE OUTCOMES:

CO1:Understand the various concept of malware analysisand their technologies used.
CO2:Possess the skills necessary to carry out independent analysis of modern malware samples using both static and dynamic analysis techniques
CO3: Understand the methods and techniques used by professional malwareanalysts
CO4:To be able to safely analyze, debug, and disassemble any malicious software by malware analysis
CO5: Understand the concept of Android malware analysis their architecture, and App development

REFERENCES

1. Michael Sikorski and Andrew Honig, “Practical Malware Analysis” by No Starch Press, 2012,ISBN: 9781593272906
2. Bill Blunden, “The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System”, Second Edition,Jones & Bartlett Publishers, 2009.
3. Jamie Butler and Greg Hoglund, “Rootkits: Subverting the Windows Kernel” by 2005, Addison-Wesley Professional, ISBN:978-0-321-29431-9
4. Bruce Dang, Alexandre Gazet, Elias Bachaalany, SébastienJosse, "Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation", 2014, ISBN: 978-1-118-78731-1
5. Victor Marak, "Windows Malware Analysis Essentials" Packt Publishing, O’Reilly, 2015, ISBN: 9781785281518
6. Ken Dunham, Shane Hartman, Manu Quintans, Jose Andre Morales, Tim Strazzere, "Android Malware and Analysis",CRC Press, Taylor & Francis Group, 2015, ISBN: 9781482252194
7. Windows Malware Analysis Essentials by Victor Marak, Packt Publishing, 2015

BC4015 SECURE SOFTWARE DESIGN AND DEVELOPMENT L T P C
3 0 2 4

COURSE OBJECTIVES:

- To fix software flaws and bugs in various software.
- To make aware of various issues like weak random number generation, information leakage, poor usability and weak or no encryption on data traffic.
- Techniques for successfully implementing and supporting network services on an enterprise scale and heterogeneous systems environment.

- Methodologies and tools to design and develop secure software containing minimum vulnerabilities and flaws.

UNIT I SECURE SOFTWARE DESIGN 8

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

UNIT II ENTERPRISE APPLICATION DEVELOPMENT 10

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

UNIT III ENTERPRISE SYSTEMS ADMINISTRATION 9

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

UNIT IV ENTERPRISE NETWORK 9

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

UNIT V DEFENDING APPLICATIONS 9

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

TOTAL: 45 PERIODS

PRACTICALS:

1. Study of various open source security tools for Application testing, Code Review, Penetration Testing, Vulnerability Assessment, Vulnerability Scanner etc.
2. Design and develop multi-tier applications for an enterprise.
3. Installation of Directory based Server and monitoring resource utilization.
4. Practicals based on network services such as DNS/DHCP/Terminal Services/Clustering/Web/Email
5. Study of SQL Injection Problem.
6. Developing applications that can defend against SQL injection problems.

TOTAL: 30 PERIODS

TOTAL:45+30=75 PERIODS

COURSE OUTCOMES:

After the completion of this course, student will be able to

CO1: Differentiate between various software vulnerabilities.
CO2: Explain the Software process vulnerabilities for an organization.
CO3: Demonstrate the Monitor resources consumption in software.
CO4: Explain the Interrelate security and software development process.
CO5: Discuss the Case study of DNS server, DHCP configuration and SQL injection attack.

REFERENCES

1. Theodor Richardson, Charles N Thies, "Secure Software Design", Jones & Bartlett Publishers, 2013

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

BC4016 SECURITY ASSESSMENT AND RISK ANALYSIS L T P C
3 0 2 4

COURSE OBJECTIVES:

- Describe the concepts of risk management
- Define and differentiate various Contingency Planning components
- Integrate the IRP, DRP, and BCP plans into a coherent strategy to support sustained organizational operations.
- Define and be able to discuss incident response options, and design an Incident Response Plan for sustained organizational operations.

UNIT I SECURITY BASICS 8

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

UNIT II THREATS AND VULNERABILITIES OF SYSTEMS & RISK MANAGEMENT 9

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

UNIT III SECURITY PLANNING 10

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

UNIT IV PHYSICAL SECURITY MEASURES, PRACTICES AND PROCEDURES **10**

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

UNIT V OPERATIONS SECURITY **8**

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

TOTAL: 45 PERIODS

PRACTICALS::

1. To audit the C/ C++ / Python code using RATS code checking tool.
2. Implement Flawfinder stand-alone script to check for calls to know potentially vulnerable library function calls.
3. Implement FindBugs standalone GUI application, or Eclipse plugin for loading custom rules set.
4. Implement pychecker stand-alone script to find bugs in the code.
5. Installation of splunk and study basic working as to stores data in its index and therefore separate database required
6. Implement splunk to discovers useful information automatically without searching manually
7. Implement splunk to converts log data into Visual graphs and reports to simplify analysis, reporting and troubleshooting
8. Assess and submit a report on cyber security risk assessment for SCADA and DCS networks.

TOTAL: 30 PERIODS

TOTAL:45+30=75 PERIODS

COURSE OUTCOMES:

After the completion of this course, student will be able to

CO1: Recommend contingency strategies including data backup and recovery and alternate site selection for business resumption planning.

CO2: Describe the escalation process from incident to disaster in case of security disaster.

CO3: Design a Disaster Recovery Plan for sustained organizational operations.

CO4: Design a Business Continuity Plan for sustained organizational operations.

CO5: Explain the concept of Operations Security and assessment of threat and vulnerability.

REFERENCES

1. Michael Whitman and Herbert Mattord, "Principles of Incident Response and Disaster Recovery", Thomson Course Technology, 2007, ISBN: 141883663X
2. http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf
3. Atle Refsdal, Bj rnar Solhaug, Ketil St len.Cyber-Risk Management, Springer, 2015

4. Martin Weiss; Michael G. Solomon, "Auditing IT Infrastructures for Compliance", Second Edition,Jones & Bartlett Learning, 2016, ISBN: 9781284090703
5. Mark Talabis and Jason Martin, "Information Security Risk Assessment Toolkit", 1st Edition, Syngres /Elsevier, 2012, ISBN: 9781597497350

BC4017 STEGANOGRAPHY AND DIGITAL WATERMARKING L T P C
3 0 2 4

COURSE 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 6

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

UNIT II STEGANOGRAPHY 10

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

UNIT III WATERMARKING 10

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 10

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

PRACTICALS:

1. Implementation of secure/Secret Communication of data

2. Experiment on claiming ownership of digital entity
3. Implementation of tracing the digital theft in cyberspace
4. Implementation of application in Block Codes
5. Implementation of universal steganalysis
6. Experiment on target steganalysis
7. Experiment on data hiding in different image types
8. Implementation of statistical steganalysis
9. Implementation of reversible data hiding
10. Implementation of Steganography in transform domain and Steganography in encrypted images

COURSE OUTCOMES:

After the completion of this course, student will be able to

CO1: Design cryptographic algorithms and carry out their implementation.
CO2: Carry out cryptanalysis on cipher.
CO3: Design and implement security protocols.
CO4: Carry out system security for various threat environments.
CO5: Explain the importance of firewall security for networks.

TOTAL: 30 PERIODS
TOTAL: 45+30=75 PERIODS

REFERENCES

1. Ingemar J. Cox, Mathew L. Miller, Jefrey A. Bloom, Jesica Fridrich, Ton Kalker, “Digital Watermarking and Steganography”, Morgan Kaufmann Publishers, New York, 2008.
2. Ingemar J. Cox, Mathew L. Miller, Jefrey A. Bloom, “Digital Watermarking”, Morgan Kaufmann Publishers, New York, 2003
3. Ingemar Cox, Mathew Miller, 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 Applications of Digital Watermarking and Content Protection”, Artech House, London, 2003.
7. Peter Wayner, “Disappearing 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. Muller, “Digital Image” Aktiengesellschaft & Co. Kg, Dec 2009.

CP4072 **BLOCKCHAIN TECHNOLOGIES** **L T P C**
3 0 2 4

COURSE OBJECTIVES:

- This course is intended to study the basics of Blockchain technology.
- During this course the learner will explore various aspects of Blockchain technology like application in various domains.

- By implementing, learners will have idea about private and public Blockchain, and smart contract.

UNIT I INTRODUCTION OF CRYPTOGRAPHY AND BLOCKCHAIN 9

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

UNIT II BITCOIN AND CRYPTOCURRENCY 9

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

UNIT III INTRODUCTION TO ETHEREUM 9

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

UNIT-IV INTRODUCTION TO HYPERLEDGER AND SOLIDITY PROGRAMMING 10

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

UNIT V BLOCKCHAIN APPLICATIONS 8

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

TOTAL: 45 PERIODS

LIST OF EXPERIMENTS:

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

TOTAL: 30 PERIODS

SUPPLEMENTARY RESOURCES:

- NPTEL online course : https://nptel.ac.in/courses/106/104/106104220/#
- Udemy: https://www.udemy.com/course/build-your-blockchain-az/
- EDUXLABS Online training :https://eduxlabs.com/courses/blockchain-technology-training/?tab=tab-curriculum

TOTAL: 75 PERIODS

COURSE OUTCOMES:

After the completion of this course, student will be able to

CO1: Understand and explore the working of Blockchain technology

CO2: Analyze the working of Smart Contracts

CO3: Understand and analyze the working of Hyperledger

CO4: Apply the learning of solidity to build de-centralized apps on Ethereum

CO5: Develop applications on Blockchain

REFERENCES:

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

BC4018	WEB SECURITY	L	T	P	C
		3	0	2	4

COURSE OBJECTIVES:

- To provide the importance of Web Security
- To discuss the fundamentals of web application authentication and session management
- To study and practice fundamental techniques in developing secure web based applications
- To identify and find the vulnerabilities of web based applications and to protect those applications from attacks
- To examine the exploiting and preventing of path traversal vulnerability

UNIT I WEB APPLICATION TECHNOLOGIES 9

Introduction – Evolution of web applications – Web application security – Core defense mechanisms – Handling user access – Handling user input – Handling attackers – Managing the application - The OWASP top ten list

Web Application Technologies : Web functionality – Encoding schemes – Mapping the Application - Enumerating the content and functionality – Analysing the application – Bypassing client side controls : Transmitting data via the client – Capturing user data – Handling client side data securely - Input Validation, Blacklist Validation - Whitelist Validation - The Defence-in-Depth Approach - Attack Surface Reduction Rules of Thumb

UNIT II WEB APPLICATION AUTHENTICATION AND SESSION MANAGEMENT 9

Web Application Authentication : Authentication Fundamentals- Two factor and Three Factor authentication - Password Based, Built in HTTP, single sign-on Custom Authentication- Secured Password based authentication: Attacks against password, Importance of password complexity – Design flaws in authentication mechanisms – Implementation flaws in authentication mechanisms – Securing authentication

Session Management: Need – Weaknesses in Session Token Generation – Weaknesses in Session Token Handling – Securing Session Management; Access Control : Access Control overview, Common vulnerabilities – attacking access controls – Securing Access Controls

UNIT III WEB SECURITY PRINCIPLES: 9

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

UNIT IV WEB APPLICATION VULNERABILITY 9

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

UNIT V EXPLOITING SYSTEMS 9

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

TOTAL: 45 PERIODS

PRACTICALS::

1. Exploration of web security in popular websites
2. Experimentation on Crawling a website
3. Implement the Vulnerability scanning
4. Implement the Cookie Stealing with cross site scripting
5. Implement the Commit identity theft
6. Implement the Website Security implementation – Apache hardening, MySQL hardening, PHP hardening
7. Implement the XSS and SQL injections
8. Experimentation on Password security
9. Experimentation on Browser security
10. Experimentation on Web application security assessment
11. Sample projects that can be given to students :
12. Experimentation on Broken Authentication and Session Management
13. Experimentation on Cross-site scripting
14. Experimentation on Insecure direct object references
15. Experimentation on Security misconfiguration
16. Experimentation on Missing function level access control
17. Experimentation on Cross-site request forgery
18. Implement using components with known vulnerabilities

COURSE OUTCOMES:

CO1: To understand common vulnerabilities plaguing today's web applications

CO2: To understand security-related issues in web based systems and applications.

CO3: To understand the fundamental security mechanisms of a Web-based system.

CO4: To be able to develop and deploy customized exploits that can bypass common defenses

CO5: To be able to evaluate a web based system with respect to its security requirements.

TOTAL: 30 PERIODS

TOTAL:45+30=75 PERIODS

REFERENCES

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

AUDIT COURSES

AX4091 ENGLISH FOR RESEARCH PAPER WRITING L T P C
2 0 0 0

COURSE OBJECTIVES:

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

UNIT I INTRODUCTION TO RESEARCH PAPER WRITING 6

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

UNIT II PRESENTATION SKILLS 6

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

UNIT III TITLE WRITING SKILLS 6

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

UNIT IV RESULT WRITING SKILLS 6

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

UNIT V VERIFICATION SKILLS 6

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

TOTAL: 30 PERIODS

COURSE OUTCOMES

CO1 –Understand that how to improve your writing skills and level of readability
CO2 – Learn about what to write in each section
CO3 – Understand the skills needed when writing a Title
CO4 – Understand the skills needed when writing the Conclusion

CO5 – Ensure the good quality of paper at very first-time submission

REFERENCES:

1. Adrian Wallwork , English for Writing Research Papers, Springer New York Dordrecht Heidelberg London, 2011
2. Day R How to Write and Publish a Scientific Paper, Cambridge University Press 2006
3. Goldbort R Writing for Science, Yale University Press (available on Google Books) 2006
4. Highman N, Handbook of Writing for the Mathematical Sciences, SIAM. Highman's book 1998.

AX4092 DISASTER MANAGEMENT L T P C
2 0 0 0

COURSE OBJECTIVES:

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

UNIT I INTRODUCTION 6

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

UNIT II REPERCUSSIONS OF DISASTERS AND HAZARDS 6

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

UNIT III DISASTER PRONE AREAS IN INDIA 6

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

UNIT IV DISASTER PREPAREDNESS AND MANAGEMENT 6

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

UNIT V RISK ASSESSMENT 6

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

TOTAL : 30 PERIODS

COURSE OUTCOMES:

CO1: Ability to summarize basics of disaster

CO2:Ability to explain a critical understanding of key concepts in disaster risk reduction and humanitarian response.

CO3: Ability to illustrate disaster risk reduction and humanitarian response policy and practice from multiple perspectives.

CO4: Ability to describe an understanding of standards of humanitarian response and practical relevance in specific types of disasters and conflict situations.

CO5: Ability to develop the strengths and weaknesses of disaster management approaches

REFERENCES:

1. Goel S. L., Disaster Administration And Management Text And Case Studies",Deep & Deep Publication Pvt. Ltd., New Delhi,2009.
2. NishithaRai, Singh AK, "Disaster Management in India: Perspectives, issues and strategies "'NewRoyal book Company,2007.
3. Sahni, Pradeep Et.Al. ," Disaster Mitigation Experiences And Reflections", Prentice Hall OfIndia, New Delhi,2001.

AX4093 CONSTITUTION OF INDIA L T P C
2 0 0 0

COURSE OBJECTIVES:

Students will be able to:

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

UNIT I HISTORY OF MAKING OF THE INDIAN CONSTITUTION

History, Drafting Committee, (Composition & Working)

UNIT II PHILOSOPHY OF THE INDIAN CONSTITUTION

Preamble, Salient Features

UNIT III CONTOURS OF CONSTITUTIONAL RIGHTS AND DUTIES

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

UNIT IV ORGANS OF GOVERNANCE

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

UNIT V LOCAL ADMINISTRATION

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

UNIT VI ELECTION COMMISSION

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

TOTAL: 30 PERIODS

COURSE OUTCOMES

Students will be able to:

- Discuss the growth of the demand for civil rights in India for the bulk of Indians before the arrival of Gandhi in Indian politics.
- Discuss the intellectual origins of the framework of argument that informed the conceptualization
- of social reforms leading to revolution in India.
- Discuss the circumstances surrounding the foundation of the Congress Socialist Party[CSP] under the leadership of Jawaharlal Nehru and the eventual failure of the proposal of direct elections through adult suffrage in the Indian Constitution.
- Discuss the passage of the Hindu Code Bill of 1956.

REFERENCES:

1. The Constitution of India,1950(Bare Act),Government Publication.
2. Dr.S.N.Busi, Dr.B. R.Ambedkar framing of Indian Constitution,1st Edition, 2015.
3. M.P. Jain, Indian Constitution Law, 7th Edn., LexisNexis,2014.
4. D.D. Basu, Introduction to the Constitution of India, LexisNexis, 2015.

AX4094	நற்றமிழ் இலக்கியம்	L T P C 2 0 0 0

UNIT I சங்க இலக்கியம் 6

1. தமிழின் துவக்க நூல் தொல்காப்பியம்
– எழுத்து, சொல், பொருள்
2. அகநானூறு (82)
- இயற்கை இன்னிசை அரங்கம்
3. குறிஞ்சிப் பாட்டின் மலர்க்காட்சி
4. புறநானூறு (95,195)
- போரை நிறுத்திய ஔவையார்

UNIT II அறநெறித் தமிழ் 6

1. அறநெறி வகுத்த திருவள்ளுவர்
- அறம் வலியுறுத்தல், அன்புடைமை, ஒப்புறவு அறிதல், ஈகை,

புகழ்

2. பிற அறநூல்கள் - இலக்கிய மருந்து
– ஏலாதி, சிறுபஞ்சமூலம், திரிகடுகம், ஆசாரக்கோவை (தூய்மையை வலியுறுத்தும் நூல்)

UNIT III **இரட்டைக் காப்பியங்கள்** **6**

1. கண்ணகியின் புரட்சி
   - சிலப்பதிகார வழக்குரை காதை
2. சமூகசேவை இலக்கியம் மணிமேகலை
   - சிறைக்கோட்டம் அறக்கோட்டமாகிய காதை

UNIT IV **அருள்நெறித் தமிழ்** **6**

1. சிறுபாணாற்றுப்படை
   - பாரி முல்லைக்குத் தேர் கொடுத்தது, பேகன் மயிலுக்குப் போர்வை கொடுத்தது, அதியமான் ஔவைக்கு நெல்லிக்கனி கொடுத்தது, அரசர் பண்புகள்
2. நற்றிணை
   - அன்னைக்குரிய புன்னை சிறப்பு
3. திருமந்திரம் (617, 618)
   - இயமம் நியமம் விதிகள்
4. தர்மச்சாலையை நிறுவிய வள்ளலார்
5. புறநானூறு
   - சிறுவனே வள்ளலானான்
6. அகநானூறு (4) - வண்டு
   நற்றிணை (11) - நண்டு
   கலித்தொகை (11) - யானை, புறா
   ஐந்திணை 50 (27) - மான்
   ஆகியவை பற்றிய செய்திகள்

UNIT V **நவீன தமிழ் இலக்கியம்** **6**

1. உரைநடைத் தமிழ்,
   - தமிழின் முதல் புதினம்,
   - தமிழின் முதல் சிறுகதை,
   - கட்டுரை இலக்கியம்,
   - பயண இலக்கியம்,
   - நாடகம்,
2. நாட்டு விடுதலை போராட்டமும் தமிழ் இலக்கியமும்,
3. சமுதாய விடுதலையும் தமிழ் இலக்கியமும்,
4. பெண் விடுதலையும் விளிம்பு நிலையினரின் மேம்பாட்டில் தமிழ் இலக்கியமும்,
5. அறிவியல் தமிழ்,
6. இணையத்தில் தமிழ்,
7. சுற்றுச்சூழல் மேம்பாட்டில் தமிழ் இலக்கியம்.

TOTAL: 30 PERIODS

தமிழ் இலக்கிய வெளியீடுகள் / புத்தகங்கள்

1. தமிழ் இணைய கல்விக்கழகம் (Tamil Virtual University)
- www.tamilvu.org
2. தமிழ் விக்கிப்பீடியா (Tamil Wikipedia)
-https://ta.wikipedia.org
3. தர்மபுர ஆதீன வெளியீடு
4. வாழ்வியல் களஞ்சியம்
   - தமிழ்ப் பல்கலைக்கழகம், தஞ்சாவூர்
5. தமிழ்கலைக் களஞ்சியம்
   - தமிழ் வளர்ச்சித் துறை (thamilvalarchithurai.com)
6. அறிவியல் களஞ்சியம்
   - தமிழ்ப் பல்கலைக்கழகம், தஞ்சாவூர்