Detailed Scheme

ACADEMIC YEAR 2020-2021

Dr. Ambedkar Institute of Technology
Bangalore

I-II (2020-2022 BATCH)

M. Tech in Cyber Forensics and Information Security

Department Of Information Science and Engineering

Dr. Ambedkar Institute of Technology
SCHEME OF TEACHING AND EXAMINATION (Autonomous)for Academic Year 2020-2021
M. Tech **in Cyber Forensics and Information Security**
Batch:2020-2022

I semester

Sl. No.	Sub Code	Subject Title	Teaching Department	Teaching hours per week			Maximum Marks allotted			Examination Credits
				Lecture	Tutorial/ Seminar/ Assignment	Practical / Project	CIE	SEE	Total	
1.	20SCF11	Probability Statistics and Queuing Theory	**MAT**	4	-	-	50	50	100	**3**
2.	20SCF12	Risk Assessment and Security Audit	ISE	4	-	-	50	50	100	**3**
3.	20SCF13	Cryptography and Network Security	ISE	4	-	-	50	50	100	**3**
4.	20SCF14	Web Applications and Web Security	ISE	4	-	-	50	50	100	**3**
5.	20SCF15X	ELECTIVE – I	ISE	4	-	-	50	50	100	**3**
6.	20SCFL16	Computer Networks and CNS Lab	ISE	-	-	3	50	50	100	**2**
7.	20SCFS17	Technical Seminar	ISE	-	2	-	50	-	50	**2**
8.	20SCF M18	Mini project/ Industry visit/ Field work	ISE	-	-	6	50	-	50	**2**
Total							**400**	**300**	**700**	**21**

Technical Seminar: Seminar on Advanced topics from refereed journals by each student.

ELECTIVE I

Sl .No	Name of the Subject	Subject Code
1	Cloud Security	20SCF151
2	Mobile And Digital Forensics	20SCF152
3	Trends in Artificial Intelligence and Soft Computing	20SCF153
4	Advances In Storage Area Networks	20SCF154

HEAD DEPT. OF INFORMATION SCIENCE & ENGG

Dr. Ambedkar Institute of Technology
SCHEME OF TEACHING AND EXAMINATION (Autonomous) Academic Year 2020-2021
M. Tech in **Cyber Forensics and Information Security**
Batch:2020-2022

II Semester

Sl. No.	Sub Code	Subject Title	Teaching Department	Teaching hours per week			Maximum Marks allotted			Examination Credits
				Lecture	Tutorial/ Seminar/ Assignment	Practical / Project	CIE	SEE	Total	
1.	20SCF21	Ethical Hacking	ISE	4	-	-	50	50	100	**3**
2.	20SCF22	Secured Programming	ISE	4	-	-	50	50	100	**3**
3.	20SCF23	Information Security Policies In Industry	ISE	4	-	-	50	50	100	**3**
4.	20SCF24	Operating System Security	ISE	4	-	-	50	50	100	**3**
5.	20SCF25X	ELECTIVE – II	ISE	4	-	-	50	50	100	**3**
6.	20SCFL26	Ethical Hacking Laboratory	ISE	-	-	3	50	50	100	**2**
7.	18RM27	Research Methodology	ISE	-	2	-	50	50	100	**2**
8.	20SCFL28	Mini project/ Industry visit/ Field work	ISE	-	-	6	50	-	50	**2**
Total							**400**	**350**	**750**	**21**

ELECTIVE-II

Sl .No	Name of the Subject	Subject Code
1	IOT Security	20SCF251
2	Mobile Device Forensics	20SCF252
3	Database Security	20SCF253
4	Storage Management And Security	20SCF254

I SEMESTER

Sub Title : PROBABILITY STATISTICS AND QUEUING THEORY		
SubCode:20SCF11	**No. of Credits:3= 3:0:0 (L-T-P)**	**No.of Lecture Hours/Week :4**
Exam Duration : 3 hours	**CIE + SEE = 50 + 50 =100**	**Total No. of Contact Hours : 52**

Course Objectives:

1.Develop analytical capability and to impart knowledge of Probability, Statistics and Queuing.

2. Apply above concepts in Engineering and Technology.

3.Acquire knowledge of Hypothesis testing and Queuing methods and their applications so as to enable them to apply them for solving real world problems

UNIT No	**Syllabus Content**	**No of Hours**
1	Axioms of probability, Conditional probability, Total probability, Baye's theorem, Discrete Random variable, Probability mass function, Continuous Random variable. Probability density function, Cumulative Distribution Function, and its properties, Two-dimensional Random variables, Joint pdf / cdf and their properties	**12**
2	Probability Distributions / Discrete distributions: Binomial, Poisson Geometric and Hyper-geometric distributions and their properties. Continuous distributions: Uniform, Normal, exponential distributions and their properties	**10**
3	Random Processes: Classification, Methods of description, Special classes, Average values of Random Processes, Analytical representation of Random Process, Autocorrelation Function, Cross-correlation function and their properties, Ergodicity, Poisson process, Markov Process and Markov chain.	**10**
4	Testing Hypothesis: Testing of Hypothesis: Formulation of Null hypothesis, critical region, level of significance, errors in testing, Tests of significance for Large and Small Samples, t-distribution, its properties and uses, F-distribution, its properties and uses, Chi-square distribution and its properties and uses, $\chi 2$ – test for goodness of fit, $\chi 2$ test for independence.	**10**
5	Symbolic representation of a Queuing Model, Poisson Queue system, Little Law, Types of Stochastic Processes, Birth-Death Process, The M/M/1 Queuing System, The M/M/s Queuing System, The M/M/s Queuing with Finite buffers.	**10**

Note 1: All units will have internal choice
Note 2: Three Assignments are evaluated for 10 marks:
Assignment – I from Units 1 and 2.
Assignment – II from Units 3 and 4
Assignment -III from Unit 5
Note 3:Subject Seminar & group activity is evaluated for 10 marks

Course Outcomes:
After the completion of the above course students will be able to:
CO1: Demonstrate use of probability and characterize probability models using probability mass (density) functions & cumulative distribution functions.
CO2: Explain the techniques of developing discrete & continuous probability distributions and its applications.
CO3: Outline methods of Hypothesis testing for goodness of fit
CO4: Define the terminology &nomenclature appropriate queuing theory and also distinguish various queuing models.

COs	**Mapping with POs**
CO1	PO3,PO4,PO7,PO9,PO10
CO2	PO2,PO3,PO4,PO9,PO12
CO3	PO2,PO3,PO4,PO9,PO12
CO4	PO2,PO3,PO4,PO9,PO12

TEXT BOOKS:

1. Probability, Statistics and Queuing Theory, V. Sundarapandian, Eastern Economy Edition, PHI Learning Pvt. Ltd, 2009.

REFERENCE BOOKS / WEBLINKS:

1. Probability & Statistics with Reliability, Queuing and Computer Applications, 2 nd Edition by Kishor. S. Trivedi , Prentice Hall of India ,2004.
2. Probability, Statistics and Random Processes, 1st Edition by P Kausalya, Pearson Education, 2013.

Course Title: RISK ASSESSMENT & SECURITY AUDIT		
Course Code: 20SCF12	**No. of Credits: 3 = 3: 0 : 0 (L–T–P)**	**No of Lecture Hours/Week:4**
Exam Duration: 3 Hours	**CIE + SEE = 50 + 50 =100**	**Total No. of Contact Hours : 52**

Course Objectives:
1.To gain the knowledge about Information Risk.
2. To discover knowledge in collecting data about organization.
3. To do various analysis on Information Risk Assessment.
4. To understand IT audit and its activities.

Unit No	**Syllabus content**	**No of Hours**
1	INTRODUCTION: What is Risk? –Information Security Risk Assessment Overview- Drivers, Laws and Regulations- Risk Assessment Frame work – Practical Approach. **Text Book1: Chapter1: Page 1-26** **Chapter2: Page 27**	**10**
2.	DATA COLLECTION: The Sponsors- The Project Team- Data Collection Mechanisms- Executive Interviews- Document Requests- IT Assets Inventories- Profile & Control Survey Consolidation. **Text Book1: Chapter3: Page 64-96**	**10**
3.	DATA ANALYSIS :Compiling Observations- Preparation of catalogs- System Risk Computation Impact Analysis Scheme- Final Risk Score **Text Book1: Chapter4: Page 105-140**	**10**
4.	RISK ASSESSMENT :System Risk Analysis- Risk Prioritization- System Specific Risk Treatment- Issue Registers- Methodology- Result- Risk Registers- Post Mortem. **Text Book1: Chapter5: Page 148-175** **Chapter6: Page 177-187** **Chapter7: Page 199-224** **Chapter8: Page 236**	**10**
5.	SECURITY AUDIT PROCESS: Pre-planning audit- Audit Risk Assessment- Performing Audit- Internal Controls Audit Evidence-Audit Testing- Audit Finding- Follow-up activities. **Text Book2: Chapter2: Page 63-105**	**12**

Note 1: All units will have internal choice
Note 2: Three Assignments are evaluated for 10 marks:
Assignment – I from Units 1 and 2.
Assignment – II from Units 3 and 4
Assignment -III from Unit 5
Note 3:Subject Seminar & group activity is evaluated for 10 marks

Course Outcomes:
After the successful completion of the course the students are able to:

CO1: Analyze the difference between Security Metrics and Audits.
CO2: Knowledge on Vulnerability Management
CO3: Know the Information Security Audit Tasks, Reports and Post Auditing Actions
CO4: Apply Information Security Assessments
CO5: Design risk management process and control practices in an audit context

COs	**Mapping with POs**
CO1:	PO1, PO2,PO3,PO4
CO2:	PO1, PO2 ,PO3,PO4
CO3:	PO1, PO2, PO3,PO4,PO5
CO4:	PO1, PO2, PO3,PO5
CO5:	PO1, PO2,PO4,PO7

TEXT BOOKS:

1. Mark Talabis, "Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis", Syngress; 1 edition, ISBN: 978-1-59749-735-0, 2012.

2. David L. Cannon, "CISA Certified Information Systems Auditor Study Guide", John Wiley & Sons, ISBN: 978-0-470-23152-4, 2009.

Course Title : **CRYPTOGRAPHY AND NETWORK SECURITY**		
Course Code: 20SCF13	**No. of Credits: 3=3 : 0 : 0 (L-T-P)**	**No. of lecture hours/week : 4**
Exam Duration : 3hours	**CIE + SEE = 50 + 50 =100**	**Total No. of Contact Hours : 52**

Course Objectives:

1. To understand the fundamentals of Cryptography .
2. To acquire knowledge on standard algorithms used to provide security.
3. To understand the various key distribution and management schemes.
4. To gain knowledge of securing data in transit across networks

UNIT No	Syllabus Content	No of Hours
1	**Classical Encryption Techniques:** Symmetric Cipher Model, Cryptography, Cryptanalysis and Brute-Force Attack, Substitution Techniques, Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, Hill Cipher, Polyalphabetic Cipher, One Time Pad (Text Book : Chapter 1:1,2,3) **Block Ciphers and the data encryption standard:** Traditional block Cipherstructure, stream Ciphers and block Ciphers, Motivation for the feistel Cipher structure, the feistel Cipher, The data encryption standard, DES encryption, DES decryption, A DES example, results, the avalanche effect, the strength of DES, the use of 56-Bit Keys, the nature of the DES algorithm, timing attacks, Block cipher design principles, number of rounds, design of function F, key schedule algorithm. (Text Book : Chapter 2: 1,2,3,4,5)	**10**
2	**Public-Key Cryptography and RSA** Principles of public-key cryptosystems. Publickey cryptosystems. Applications for public-key cryptosystems, requirements for public-key cryptosystems. public-key cryptanalysis. The RSA algorithm, description of the algorithm, computational aspects, the security of RSA. Text Book : Chapter-8:1,2 **Other Public-Key Cryptosystems:** Diffie-hellman key exchange: The algorithm, key exchange protocols, man in the middle attack, Elgamal Cryptographic systems, Elliptic curve arithmetic: Abelian groups, elliptic curves over real numbers, elliptic curves over Zp, elliptic curves over GF(2m) Elliptic curve cryptography: Analog of Diffie-hellman key exchange, Elliptic curve encryption/decryption, security of Elliptic curve cryptography. Pseudorandom number generation: PRNG based on RSA PRNG Based on ECC.Text Book : Chapter-9:1,2,3,4,5	**10**

3	**Key Management and Distribution:**Symmetric key distribution using Symmetric encryption:A key distribution scenario, Hierarchical key control, session key lifetime, a transparent key control scheme, Decentralized key control, controlling key usage,Symmetric key distribution using asymmetric encryption: simple secret key distribution, secret key distribution with confidentiality and authentication, A hybrid scheme.Distribution of public keys: public announcement of public keys, publicly available directory, public key authority, public keys certificates.X-509 certificates: Certificates, X-509 version 3. Text Book : Chapter-13: 1,2,3,4,5 **User Authentication:**Remote user Authentication principles: Mutual Authentication, one way Authentication.Remote user Authentication using Symmetric encryption:Mutual Authentication, one way Authentication. **Kerberos:** Motivation , Kerberos version 4, Kerberos version 5:Differences between version 4 and 5 Remote user Authentication using Asymmetric encryption: Mutual Authentication, one way Authentication Federated identity management: identity management, identity federation Text Book : Chapter-14: 1,2,3,4 ,5	**10**
4	**Transport –Level Security** Web Security Considerations: Web Security Threats, Web Traffic Security Approaches.Secure Sockets Layer: SSL Architecture, SSL Record Protocol, Change Cipher Spec Protocol, Alert Protocol, and shake Protocol, Cryptographic Computations.Transport Layer Security:Version Number, Message Authentication Code, Pseudorandom Functions, Alert Codes, Cipher Suites, Client Certificate Types, Certificate Verify And Finished Messages, Cryptographic Computations, Padding. HTTPS :Connection Initiation, Connection Closure. Secure Shell (SSH) Transport Layer Protocol, User Authentication Protocol, Connection Protocol. Text Book : Chapter-15: 1,2,3,4,5	**10**
5	**Electronic Mail Security:**Pretty good privacy: Notation, Operational description S/MIME:RFC5322, Multipurpose internet mail extensions, S/MIME functionality, S/MIME messages Domain keys identified mail: Internet Mail Architecture, E-Mail threats, DKIM strategy, DKIM functional flow Text Book : Chapter-17: 1,2,3 **IP Security:**IP Security overview: Applications of IPsec, benefits of IPsec, Routing applications, IPsec documents, IPsec services, transport and tunnel modes IP Security policy: Security associations, Security associations database, Security policy database, IP traffic processing, Encapsulating Security payload: ESP format, encryption and authentication algorithms, Padding, Anti replay service, transport and tunnel modes Combining security associations: Authentication plus confidentiality, basic combinations of	**12**

	security associations, Internet key exchange:key determinations protocol, header and payload formats Text Book : Chapter-18: 1,2,3,4,5	

Note 1: All units will have internal choice

Note 2: Three Assignments are evaluated for 10 marks:

Assignment – I from Units 1 and 2.

Assignment – II from Units 3 and 4

Assignment -III from Unit 5

Note 3:Subject Seminar & group activity is evaluated for 10 marks

Course Outcomes:

After the completion of the course students will be able to

CO1: Analyze the vulnerabilities in any computing system and hence be able to design a security solution.

CO2: Identify the security issues in the network and resolve it.

CO3:Apply key management and distribution techniques .

CO4: Analyze security mechanisms at various layers of network model.

COs	Mapping with PO's
CO1	PO1,PO2,PO3,PO4
CO2	PO1,PO2,PO3,PO4
CO3	PO1,PO2,PO3,PO4,PO5
CO4	PO1,PO2,PO3,PO4,PO5

TEXT BOOK : BOOKS:

1. William Stallings: Cryptography and Network Security Principles and Practice, Pearson 6th edition. 2013

REFERENCE BOOKS / WEBLINKS:

1. V K Pachghare: Cryptography and Information Security, PHE ,2013.

Course Title :WEB APPLICATION AND WEB SECURITY		
Course code : 20SCF14	**No. of Credits:3=3: 0 : 0 (L-T-P)**	**No.of Lecture Hours/Week: 4**
Exam Duration : 3 hours	**CIE + SEE = 50 + 50 =100**	**Total No. of Contact Hours : 52**

Course Objectives:

1. Web applications vulnerability and malicious attacks.
2. Basic web technologies used for web application development.
3. Basic concepts of Mapping the application.
4. Illustrate different attacking illustrations.
5. Basic concepts of Attacking.

Unit No.	**Syllabus Content**	**No. of Hours**
1	Web Application (In) security: The Evolution of Web Applications, Common Web Application Functions, Benefits of Web Applications, Web Application Security. Core Defense Mechanisms: Handling User Access Authentication, Session Management, Access Control, Handling User Input, Varieties of Input Approaches to Input Handling, Boundary Validation. Multistep Validation and Canonicalization: Handling Attackers, Handling Errors, Maintaining Audit Logs, Alerting Administrators, Reacting to Attacks.**Chapter 1: Page 1-13** **Chapter 2: Page 15-32**	10
2	Web Application Technologies: The HTTP Protocol, HTTP Requests, HTTP Responses, HTTP Methods, URLs, REST, HTTP Headers, Cookies, Status Codes, HTTPS, HTTP Proxies, HTTP Authentication, Web Functionality, Server-Side Functionality, ClientSide Functionality, State and Sessions, Encoding Schemes, URL Encoding, Unicode Encoding, HTML Encoding, Base64 Encoding, Hex Encoding, Remoting and Serialization Frameworks.**Chapter 3: Page 35-59**	09
3	Mapping the Application: Enumerating Content and Functionality, Web Spidering, User-Directed Spidering, Discovering Hidden Content, Application Pages Versus Functional Paths, Discovering Hidden Parameters, Analyzing the Application, Identifying Entry Points for User Input, Identifying Server-Side Technologies, Identifying Server-Side Functionality, Mapping the Attack Surface. **Chapter 4: Page 61-91**	12
4	Attacking Authentication: Authentication Technologies, Design Flaws in Authentication Mechanisms, Bad Passwords, Brute-Forcible Login, Verbose Failure Messages, Vulnerable Transmission of Credentials, Password Change, Functionality, Forgotten Password Functionality, “Remember Me” Functionality, User Impersonation, Functionality Incomplete, Validation of Credentials, Nonunique Usernames, Predictable Usernames, Predictable Initial Passwords, Insecure Distribution of Credentials. Attacking Access Controls: Common Vulnerabilities, Completely Unprotected, Functionality Identifier-Based Functions, Multistage Functions, Static Files, Platform Misconfiguration, Insecure Access Control Methods.**Chapter 6:page 133-154, Chapter 8: page 217-223**	09

5	Attacking Data Stores: Injecting into Interpreted Contexts, Bypassing a Login, Injecting into SQL, Exploiting a Basic Vulnerability Injecting into Different Statement Types, Finding SQL Injection Bugs, Fingerprinting the Database, The UNION Operator, Extracting Useful Data, Extracting Data with UNION, Bypassing Filters, Second-Order SQL Injection, Advanced Exploitation Beyond SQL Injection: Escalating the Database Attack, Using SQL Exploitation Tools, SQL Syntax and Error Reference, Preventing SQL Injection **Chapter 7: Page no 237-299**	12

Note 1: All units will have internal choice

Note 2: Three Assignments are evaluated for 10 marks:

Assignment – I from Units 1 and 2.

Assignment – II from Units 3 and 4

Assignment -III from Unit 5

Note 3:Subject Seminar & group activity is evaluated for 10 marks

Course Outcomes:

After the completion of the course students will be able to

CO1: Achieve Knowledge of web applications vulnerability and malicious attacks.

CO2: Apply the basic web technologies used for web application development

CO3: Analyze the basic concepts of Mapping the application.

CO4: Able to illustrate different attacking illustrations.

CO5: Basic concepts of Attacking Data Stores.

COs	**Mapping with POs**
CO1	PO1,PO2, PO4,PO5,PO7
CO2	PO1,PO2, PO4,PO5
CO3	PO1, PO2,PO4,PO5,
CO4	PO1,PO2,PO3, PO4,
CO5	PO1,PO2, PO4,PO5, PO7

TEXT BOOK:

1. The Web Application Hacker's Handbook: Finding And Exploiting Security DefyddStuttard, Marcus Pinto Wiley Publishing, Second Edition.

REFERENCE BOOKS:

1. Professional Pen Testing for Web application, Andres Andreu, Wrox Press.

2. Carlos Serrao, Vicente Aguilera, Fabio Cerullo, Web Application Security Springer; 1st Edition

3. Joel Scambray, Vincent Liu, Caleb Sima ,"Hacking exposed, McGraw-Hill; 3rd Edition, (October, 2010).

4. OReilly Web Security Privacy and Commerce 2nd Edition 2011.

5. Software Security Theory Programming and Practice, Richard sinn, Cengage Learning.

6.Database Security and Auditing, Hassan, Cengage Learning

ELECTIVE –I

Sub Title : CLOUD SECURITY		
Sub Code: 20SCF151	**No. of Credits:3=3: 0 : 0 (L-T-P)**	**No.of Lecture Hours/Week: 4**
Exam Duration : 3 hours	**CIE + SEE = 50 + 50 =100**	**Total No. of Contact Hours : 52**

Course Objectives:

1. Fundamental security concepts and architectures that serve as building blocks to database security
2. Concepts of user account management and administration, including security risks
3. To use current database management system to design and configure the user and data permissions.
4. Operational components necessary to maximize database security using various security models

Unit No.	Syllabus Content	No. of Hours
1	**Cloud Computing Fundamentals**:Essential Characteristics-On-Demand Self-Service, BroadNetwork Access, Location-Independent Resource Pooling, Rapid Elasticity, Measured Service. Architectural Influences-High-Performance Computing, Utility and Enterprise Grid Computing, Autonomic Computing, Service Consolidation, Horizontal Scaling, Web Services, High-Scalability Architecture. Technological Influences-Universal Connectivity, Commoditization, Excess Capacity, Open-Source Software, Virtualization. Operational Influences-Consolidation, Outsourcing. Chap- 1	10
2	**Cloud Computing Architecture:**Cloud Delivery Models- Iaas, Paas, Saas. Cloud Deployment Models- Public Clouds, Community Clouds, Private Clouds, Hybrid Clouds. Expected Benefits- Flexibility and Resiliency, Reduced Costs, Centralization of Data Storage, Reduced Time to Deployment, Scalability Chap- 2	10
3	**Cloud Computing Software Security Fundamentals**:Cloud Information Security Objectives- Confidentiality, Integrity, and Availability.Cloud Security Services-Authentication, Authorization, Auditing, Accountability. Relevant Cloud Security Design –Principles, Least Privilege, Separation of Duties, Cloud Security Services. Relevant Cloud Security Design Principles-Secure Cloud Software Requirements . Secure Cloud Software Testing. Cloud Computing and Business Continuity Planning/Disaster Recovery. Chap- 3	11

4	**Cloud Computing Risk Issues:**The CIA Triad - Privacy and Compliance Risks, Threats to Infrastructure, Data, and Access Control Common Threats and Vulnerabilities, Cloud Service Provider Risks. Chap- 4	11
5	**Cloud Computing Security Challenges & Architecture**:Security Policy Implementation- Policy Types, Computer Security Incident Response Team. Virtualization Security Management- Virtual Threats, VM Security Recommendations, VM-Specific Security Techniques. Cloud Computing Security Architecture- Architectural Considerations, Identity Management and Access Control. Chap- 5,6	10

Note 1: All units will have internal choice
Note 2: Three Assignments are evaluated for 10 marks:
Assignment – I from Units 1 and 2.
Assignment – II from Units 3 and 4
Assignment -III from Unit 5
Note 3:Subject Seminar & group activity is evaluated for 10 marks

Course Outcomes:
After the completion of the course students will be able to

CO1: Carry out a risk analysis for a large database
CO2: Implement identification and authentication procedures, fine-grained access control and data encryption techniques.
CO3:Set up accounts with privileges and roles
CO4:Audit accounts and the database system

COs	**Mapping with POs**
CO1	PO1,PO2, PO4,PO5,PO7
CO2	PO1,PO2, PO4,PO5
CO3	PO1, PO2,PO4,PO5,
CO4	PO1,PO2,PO3, PO4,
CO5	PO1,PO2, PO4,PO5, PO7

Text Book :

1. Cloud Security- A Comprehensive Guide to Secure Cloud Computing by Ronald L. Krutz, Russell Dean Vines

Sub Title : MOBILE AND DIGITAL FORENSICS		
Sub Code: 20SCF152	**No. of Credits:3=3: 0 : 0 (L-T-P)**	**No.of Lecture Hours/Week:** **4**
Exam Duration : **3 hours**	**CIE + SEE = 50 + 50 =100**	**Total No. of Contact Hours : 52**

Course Objectives

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

Unit No.	**Syllabus Content**	**No. of Hours**
1	Overview of wireless technologies and security: Personal Area Networks, Wireless Local Area Networks, Metropolitan Area Networks, Wide Area Networks. **TextBook1: Chapter1: Page1-10**	10
2	Wireless threats, vulnerabilities and security: Wireless LANs, War Driving, War Chalking, War Flying, Common Wi-fi security recommendations, PDA Security, Cell Phones and Security, Wireless DoS attacks, GPS Jamming, Identity theft. **TextBook1: Chapter2: Page13-35**	09
3	Wireless crime fighting; Wireless crime prevention techniques, police use of wireless devices, personal security and RFID, wireless honeypots. **TextBook1: Chapter3: Page43-49**	12
4	Digital forensic principles and wireless forensics: Cyber crime forensic principles, Investigating cyber crime, Network forensics in a wireless environment, 802.11 Forensics, PDA forensics, Cell phone forensics. **TextBook1: Chapter4: Page51-106**	09
5	The wireless future: Introduction, new Twists, pervasive computing and cultural shifts, wireless shifts and trends, new functionalities for wireless devices, The home element, Relationships, virtual communities and beyond, city-sized hotspots, security and privacy. **TextBook1: Chapter5: Page127-147**	12

Course Outcomes:

After the completion of the course students will be able to

CO1: Understand the definition of computer forensics fundamentals

CO2: Describe the types of computer forensics technology.

CO3: Analyze various computer forensics systems.

CO4: Illustrate the methods for data recovery, evidence collection and data seizure

COs	**Mapping with POs**
CO1	PO1,PO2, PO4,PO5,PO7
CO2	PO1,PO2, PO4,PO5
CO3	PO1, PO2,PO4,PO5,
CO4	PO1,PO2,PO3, PO4,
CO5	PO1,PO2, PO4,PO5, PO7

TEXT BOOK:

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

REFERENCES:

1. Iosif I. Androulidakis, “ Mobile phone security and forensics: A practical approach”, Springer publications, 2012 .

2. Andrew Hoog, “ Android Forensics: Investigation, Analysis and Mobile Security for Google Android”, Elsevier publications, 2011.

3. Angus M.Marshall, “ Digital forensics: Digital evidence in criminal investigation”, John – Wiley and Sons, 2008.

Course Title : TRENDS IN ARTIFICIAL INTELLIGENCE AND SOFT COMPUTING		
CourseCode: 20SCF153	**No. of Credits:3=3 : 0 : 0 (L-T-P)**	**No. of lecture hours/week : 4**
Exam Duration : 3 hours	**CIE + SEE= 50+50 =100**	**Total No. of Contact Hours :52**

Course Objectives

1. Describe Artificial Intelligence ,its utility and intelligent agents
2. Use and implement search techniques
3. Use knowledge representation techniques for problem solving
4. Describe and apply Fuzzy systems to various problem domains
5. Describe and apply GA to different problem domains

UNIT No	**Syllabus Content**	**No of Hours**
1	Role of AI in Engineering, AI in daily life, Intelligence and AI, Different Task Domains of AI, History and Early Works of AI, History of AI, Programming Methods, Limitaions of Ai, Agent, Performance Evaluation, Task environment of an Agent, Agents Classification, Agent Architecture Logic Programming, Logic Representation, Propositional Logic, Predicate Logic and Predicate Calculus, Horn Clauses, Well formd Formula, Computable functions and predicate, Quantifiers, Universe of discourse, Applications of Predicate Logic, Unification, Resolution, Conjuctive Normal Form, conversion to normal form or clausal form .**Text1:Ch1,Ch2,Ch3**	**10**
2	Fundamental Problem of Logic: Logic Inadequacy: Fundamental Problem of Logic- Monotonicity wuith “Flying Penguin” example, General disadvantage of monotonicity property in logic , logic in search space problem, logic in decidability and Incompleteness, Logic in Uncertainty Modelling, Knowledge representation: Knowledge, Need to represent knowledge, Knowledge representation with mapping scheme, properties of a good knowledge base system, Knowledge representation issues, AND-OR graphs, Types of knowledge, Knowledge representation schemes, , semantic nets, Frames, conceptual graphs, conceptual dependence theory, script, weak and strong slot filler. Reasoning: Types of Reasoning, Methods of reasoning, Application of Reasoning, Forward and Backward Reasoning **Text1:Ch4,Ch6,Ch7.1-7.4**	**12**
3	Search Techniques: Search, Representation techniques, Categories of Search, Disadvantage of state space search, Issues in design of search programs, General Search examples, Classification of search diagram representation, Hill climbing method and Hill climbing search ,Simulates Annealing, Best-First Search, Branch and Bound Search, A search Game Playing: Two player games, Minmax Search, Complexity of Minmax algorithm, Alpha-Beta Pruning Planning: Necessity of planning, Components of Planning, Planning Agents, Plan- gererating schemes,	**10**

	Algorithm for planning, Planning Representation with STRIPS, BlOCKS WORLD, difficulties with planning. **Text1:Ch8,Ch9,Ch10,Ch11**	
4	Fuzzy Sets and Uncertainties: Fuzzy set and fuzzy logic, set and fuzzy operators, , Extended fuzzy operations, Fuzzy relations, Properties of fuzzy relations, Fuzzy system and design, Linguistic hedges, Syntax for IF and Then rules, , Types of fuzzy rule based system, Fuzzy linguistic controller, Fuzzy Inference, Graphical techniques of Inference, How, Fuzzy logic is used, Fuzzification, De-fuzzification. Unique features of Fuzzy Logic, Application of Fuzzy Logic, Fuzzy logic uncertainty and probability, Advantages and Limitations of Fuzzy logic and Fuzzy Systems.**Text1:Ch5**	**10**
5	Advancement of AI: Expert System, Expert System structure, Knowledge acquisition,Knowledge representation, Inference control mechanism, User interface, Expert System Shell, Knowledge Representation, Inference Mechanism, Developer Interface and User Interface, Characteristics of Expert system, Advantages of an expert system, Production System, Artificial Neural Networks, : Characteristics of Neural Networks, Architecture of neural networks, Types of neural networks, Application of neural networks. **Text1:Ch12**	**10**

Note 1: All units will have internal choice
Note 2: Three Assignments are evaluated for 10 marks:
Assignment – I from Units 1 and 2.
Assignment – II from Units 3 and 4
Assignment -III from Unit 5
Note 3:Subject Seminar & group activity is evaluated for 10 marks

Course Outcomes:

CO1:Design intelligent agents for problem solving, reasoning, planning, decision making, and learning.

CO2:Apply AI technique to current applications.

CO3:Apply Problem solving, knowledge representation, reasoning, and learning techniques to solve real world problems

CO4:Design and build expert systems for various application domains.

CO5:Apply Soft Computing techniques such as neural networks, fuzzy logic to solve problems in various application domains

COs	**Mapping with PO's**
CO1	PO1,PO2,PO3
CO2	PO1,PO2,PO3
CO3	PO1,PO2,PO3
CO4	PO2,PO3,PO4
CO5	PO2,PO3,PO4

Text Books:

1. Anindita Das Battacharjee, Artificial Intelligence and Soft computing for Beginners, Shroff Publishers, 2nd edition

REFERENCE BOOKS/WEBLINKS

1. Elaine Rich,Kevin Knight, Shivashanka B Nair:Artificial Intelligence, Tata CGraw Hill 3rd edition 2013.
2. Stuart Russel, Peter Norvig: Artificial Intelligence A Modern Approach, Pearson 3rd edition.
3. Neural Networks, Fuzzy Logic and Genetic Algorithms by S. Rajasekaran, G. A. Vijayalakshmi Pai PHI publication
4. Nils J. Nilsson: “Principles of Artificial Intelligence”, Elsevier, ISBN-13: 9780934613101

Sub Title : ADVANCES IN STORAGE AREA NETWORKS		
CourseCode: 20SCF154	**No. of Credits:3=3 : 0 : 0 (L-T-P)**	**No. of lecture hours/week : 4**
Exam Duration : 3 hours	**CIE + SEE= 50+50 =100**	**Total No. of Contact Hours :52**

Course Objectives:

1. To understand the fundamentals of storage architecture along with storage virtualization.
2. To understand the metrics used for designing storage area networks.
3. To enable the students to understand RAID concepts.
4. To appreciate the use of cables technologies used in SAN technology.

Unit No.	**Syllabus Content**	**No. of Hours**
1	**Introduction:** Server Centric IT Architecture and its Limitations; Storage – Centric IT Architecture and its advantages. Case study: Replacing a server with Storage Networks The Data Storage and Data Access problem; The Battle for size and access. Intelligent Disk Subsystems: Architecture of Intelligent Disk Subsystems; Hard disks and Internal I/O Channels; JBOD, Storage virtualization using RAID and different RAID levels; Caching: Acceleration of Hard Disk Access; Intelligent disk subsystems, Availability of disk subsystems. **Sections: 1.1-1.3, 2.1-2.8**	12
2	**I/O Techniques:** The Physical I/O path from the CPU to the Storage System; SCSI; Fiber Channel Protocol Stack; Fibre Channel SAN; IP Storage. Network Attached Storage: The NAS Architecture, The NAS hardware Architecture, The NAS Software Architecture, Network connectivity, NAS as a storage system. File System and NAS: Local File Systems; Network file Systems and file servers; Shared Disk file systems; Comparison of fibre Channel and NAS. **Sections: 3.1-3.5, 4.1-4.5**	10
3	**Storage Virtualization:** Definition of Storage virtualization ; Implementation Considerations; Storage virtualization on Block or file level; Storage virtualization on various levels of the storage Network; Symmetric and Asymmetric storage virtualization in the Network. **Sections: 5.3-5.7**	10
4	**Applications of Storage Network:** Definition of the Term ‘Storage Network’, Storage Sharing, Availability of Data, Adaptability and Scalability of IT Systems, General Conditions for Backup Network Backup Services Components of Backup Servers, Backup clients **Sections: 6.1-6.4, 7.1-7.4**	10
5	**Management of Storage Network:** System Management, Requirement of management System, Support by Management System, Management Interface, Standardized Mechanisms, Property Mechanisms, In-band Management, out-of-band management. **Sections: 10.1-10.4**	10

Note 1: All units will have internal choice
Note 2: Three Assignments are evaluated for 10 marks:
Assignment – I from Units 1 and 2.
Assignment – II from Units 3 and 4
Assignment -III from Unit 5
Note 3:Subject Seminar is evaluated for 10 marks

Course Outcomes:
After the completion of course, the students will be able to:

CO1: Identify the need for storage networks and its advantages.
CO2: Recognize various RAID levels.
CO3: Apply the concept of storage virtualization and recognize steps for Business continuity planning in an Enterprise.
CO4: Analyze SAN architecture along with the use of cables technologies.
CO5: Realize the concept of management of storage network.

COs	**Mapping with POs**
CO1	PO1, PO2, PO12
CO2	PO1, PO2
CO3	PO1,PO2,PO11
CO4	PO1,PO2,PO12
CO5	PO1, PO2,PO11, PO12

TEXT BOOKS:

1. Ulf Troppens, Rainer Erkens and Wolfgang Muller: Storage Networks Explained, Wiley India, 2013.

REFERENCE BOOKS/WEB LINKS:

1.Robert Spalding: “Storage Networks The Complete Reference”, Tata McGraw-Hill, 2011.
2. Marc Farley: Storage Networking Fundamentals – An Introduction to Storage Devices, Subsystems, Applications, Management, and File Systems, Cisco Press, 2005.
3. Richard Barker and Paul Massiglia: “Storage Area Network Essentials A CompleteGuide to understanding and Implementing SANs”, Wiley India, 2006

Course Title : COMPUTER NETWORKS AND CNS LABORATORY		
CourseCode: 18SCNL16	**No. of Credits:2= 0:0: 2.0 (L-T-P)**	**No. of lecture hours/week : 3**
Exam Duration : 3 hours	**CIE + SEE = 50 + 50 =100**	

Course objectives:

1. To learn Concepts of fundamental protocols.
2. To acquire knowledge of implementation concepts in error detections.
3. To understand the fundamentals of Cryptography through practical implementation.
4. To implement standard algorithms used to provide confidentiality and integrity.

Implement the following using C/C++ /JAVA or equivalent with LINUX/Windows environment:

1. Write a program to transfer the contents of a requested file from Server to the Client using TCP/IP Sockets.
2. Implement Distance Vector Routing algorithm.
3. Write a program for implementing the Error Detection Technique while data transfer in unreliable network code using CRC (16-bits) Technique.
4. Write a program to implement Caesar substitution cipher .
5. Write a program to implement rail fence transposition cipher .
6. Write a program to implement vegener polyalphabetic cipher.
7. Write a program to implement RSA encryption and decryption algorithms .
8. Write a program to implement Diffie-Hellman Key Exchange algorithm.
9. Consider an alphanumeric data, encrypt and Decrypt the data using advanced encryption standards and verify for the correctness.
10. Implement secure hash algorithm for Data Integrity. Implement MD5 and SHA-1 algorithm, which accepts a string input, and produce a fixed size number -128 bits for MD5; 160 bits for SHA-1, this number is a hash of the input. Show that a small change in the input results in a substantial change in the output.

Simulation Programs using OPNET /NS2/NS3/NCTUNS/Packet Tracer or any other equivalent software

11. Simulate a 3 node point to point network with duplex links between them. Set the Queue size and vary the bandwidth and find the number of packets dropped.

12. Simulate a four node point-to-point network with the links connected as follows: n0 – n2, n1 – n2 and n2 – n3. Apply TCP agent between n0-n3 and UDP between n1-n3. Apply relevant applications over TCP and UDP agents changing the parameter and determine the number of packets sent by TCP / UDP.

Note: In the examination the student has to answer one question from a lot of 12 questions.

Course Outcomes:

After completing the course the students are able to:

CO1: Design client server applications using socket programming API.

CO2: Implement routing , error detection algorithms.

CO3: Analyze the network performance based on simulation results .

CO4: Design and implement ciphers.

COs	**Mapping with POs**
CO1	PO2, PO3
CO2	PO2, PO3,PO4
CO3	PO2, PO3,PO4
CO4	PO2, PO3,PO4

Course Title : TECHNICAL SEMINAR		
CourseCode: 20SCFS17	No. of Credits:2= 0:2:0 (L-T-P)	No. of lecture hours/week
Exam Duration : 3 hours	CIE = 50	

Course Title : MINI PROJECT/INDUSTRY VISIT/FIELD WORK		
CourseCode: 20SCFM18	No. of Credits:2= 0:0:6 (L-T-P)	No. of lecture hours/week :
Exam Duration : 3 hours	CIE = 50	

II SEMESTER

Course Title: ETHICAL HACKING		
Course Code: 20SCF21	No. of Credits:3 = 3: 0 : 0 (L–T–P)	No of Lecture Hour/week: 4
Exam Duration: 3 Hours	CIE + SEE = 50 + 50 =100	Total No. of Contact Hours : 52

Course Objectives:

- Learn aspects of security, importance of data gathering, foot printing and system hacking.
- Learn tools and techniques to carry out a penetration testing.
- How intruders escalate privileges
- Explain Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation.
- Compare different types of hacking tools..

Unit No	Syllabus Content	No of Hours
1	Casing the Establishment: What is foot printing, Internet Foot printing, Scanning, Enumeration, basic banner grabbing, Enumerating Common Network services. Case study: Network Security Monitoring. **Text Book2: Chapter1:Page 7-42:Chapter2: Page 43-77, Chapter3: Page 79-148**	10
2.	Securing permission: Securing file and folder permission, Using the encrypting file system, Securing registry permissions. Securing service: Managing service permission, Default services in windows 2000 and windows XP. Unix: The Quest for Root, Remote Access vs Local access, Remote access, Local Access, After Hacking root. **Text Book2: Chapter5:Page 224-307**	10
3.	Dial-up, PBX, Voicemail and VPN hacking, Preparing to dial up, War-Dialing, BruteForce Scripting PBX hacking, Voice mail hacking, VPN hacking, Network Devices: Discovery Autonomous System Lookup, Public Newsgroups, Service Detection, Network Vulnerability, Detecting Layer 2 Media. **Text Book2: Chapter6:Page 315-369,Chapter7: Page 387-439**	10
4.	Wireless Hacking: Wireless Foot printing, Wireless Scanning and Enumeration, Gaining Access, Tools that exploiting WEP Weakness, Denial of Services Attacks, Firewalls: Firewalls landscape, Firewall Identification-Scanning Through firewalls, packet Filtering, Application Proxy Vulnerabilities, Denial of Service Attacks, Motivation of Dos Attackers, Types of DoS attacks, Generic Dos Attacks, UNIX and Windows DoS **Text Book2: Chapter8:Page 445-466,Text Book1: Chapter11: Page 459-479, Chapter12: Page 483-504**	11
5.	Remote Control Insecurities: Discovering Remote Control Software, Connection, Weakness.VNC, Microsoft Terminal Server and Citrix ICA, Advanced Techniques Session Hijacking, Back Doors, Trojans,	11

	Cryptography, Subverting the systems Environment, Social Engineering, Web Hacking, Web server hacking web application hacking, Hacking the internet Use, Malicious Mobile code, SSL fraud, E-mail Hacking, IRC hacking, Global countermeasures to Internet User Hacking **Text Book1: Chapter13: Page 511-526, Chapter14: Page 529-563, Chapter15: Page 565,Chapter16: Page 601-651**	

Note 1: All units will have internal choice

Note 2: Three Assignments are evaluated for 10 marks:

Assignment – I from Units 1 and 2.

Assignment – II from Units 3 and 4

Assignment -III from Unit 5

Note 3:Subject Seminar is evaluated for 10 marks

Course Outcomes: After the successful completion of the course the students are able to

CO1: Explain aspects of security, importance of data gathering, foot printing and system hacking

CO2: Explain aspects of security, importance of data gathering, foot printing and system hacking.

CO3: Demonstrate how intruders escalate privileges.

CO4: Demonstrate how intruders escalate privileges

CO5: Demonstrate how intruders escalate privileges.

COs	**Mapping with POs**
CO1	PO1, PO2
CO2	PO1, PO2
CO3	PO1, PO2
CO4	PO1, PO4
CO5	PO1, PO2

TEXT BOOKS:

1. Stuart McClure, Joel Scambray and Goerge Kurtz, Hacking Exposed 7: Network Security Secrets & Solutions, 2nd Edition, Tata Mc Graw Hill Publishers, 2010.

2. Stuart McClure, Joel Scambray and Goerge Kurtz, “Hacking Exposed Network Security Secrets & Solutions”, 6th Edition, Tata Mc Graw Hill Publishers, 2010.

3. Bensmith, and Brian Komer, Microsoft Windows Security Resource Kit, Prentice Hall

REFERENCE BOOKS/WEB LINKS

1.Stuart McClure, Joel Scambray and Goerge Kurtz, “Hacking Exposed Network Security Secrets & Solutions”, 6th Edition, Tata Mc Graw Hill publishers, 2010.

2. Rafay Baloch, “A Beginners Guide to Ethical Hacking”

3.Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, “Gray Hat Hacking The Ethical Hackers Handbook”, 3rd Edition, McGraw-Hill Osborne Media paperback(January 27, 2011)

Course Title : SECURED PROGRAMMING		
Course Code: 20SCF22	**No. of Credits:3=3 : 0 : 0 (L-T-P)**	**No.of Lecture Hours/Week: 4**
Exam Duration : 3 hours	**CIE + SEE = 50 + 50 =100**	**Total No. of Contact Hours : 52**

Course Objectives:

1. Understand the basics of secure programming.
2. Demonstrate the most frequent programming errors leading to software vulnerabilities.
3. Identify and analyze security problems in software.
4. Understand how to protect against security threats and software vulnerabilities.

Unit No..	Syllabus Content	No of Hours
1	Validating all input & Designing secure programs: Command line and environment variables, File descriptors, names and contents, Web based application inputs, Locale selection and character encoding, Filtering represent able URIs, preventing cross site malicious input content, Forbidding HTTP Input to perform non-queries. Good security design principles: Securing the interface, separation of data and control. Minimize privileges: Granted, time, modules, resources etc, Using chroot, careful use of setuid/setgid, Safe default value and load initializations. Avoid race conditions, Trustworthy channels and trusted path, Avoiding semantics and algorithmic complexity attacks. **Text Book 2: Chapter 5: 5.1 - 5.12, Chapter 7: 7.1 -7.17**	**11**
2	Declarations and Initializations and Expressions: Declare objects with appropriate storage durations, Identifier declaration with conflict linkage classifications, Using correct syntax for declaring flexible array member, Avoiding information leakage in structure padding, Incompatible declarations of same function or object. Dependence on evaluation order for side effects: Reading uninitialized memory and dereferencing null pointers, Modifying objects with temporary lifetime, Accessing variable through (pointer) incompatible type, Modifying constant objects and comparing padding data. **Text Book 1: Chapter 3: 3.1,3.3,3.5,3.6,3.7, Chapter 4:4.1,4.3-4.10**	**10**
3	Integers and Floating Points: Wrapping of unsigned integers, Integer conversions and misrepresented data, Integer overflow and divide by zero errors, Shifting of negative numbers, Using correct integer precisions, Pointer conversion to integer and vice versa. Floating point values for counters: Domain and range errors in math functions, Floating point conversions and preserving precision. **Text Book 1: Chapter 5: 5.1-5.7,Chapter 6:6.1,6.2,6.4**	**11**
4	Arrays , Strings and Memory Management: Out of bounds subscripts and valid length arrays, Comparing array pointers, Pointer arithmetic for non-array object, scaled integer, Modifying string literals, Space allocation for strings (Null terminator), Casting large integers as unsigned chars,	**10**

	Narrow and wide character strings and functions. Accessing freed memory: Freeing dynamically allocated memory, Computing memory allocation for an object, Copying structures containing flexible array members, Modifying object alignment by using realloc. **Text Book 1: Chapter 7: 7.1,7.3,7.4,7.6,Chapter 8: 8.1,8.2,8.4,8.6, Chapter 9: 9.1,9.2,9.3,9.5,9.6**	
5	I/O, Signals and Error Handing: User input and format strings, Opening an pre-opened file, Performing device operations appropriate for files, Dealing with EOF, WEOF, Copying FILE object, Careful use of fgets, fgetws, getc, putc, putwc. Use of fsetops and fgetops, Accessing closed files. Using asynchronous safe functions and signal handlers: Shared objects and signal handlers, Using signal() within interruptible signal handlers, Returning computation exception signal handler. Using errno: check and set, Depending upon indeterminate values of errno, Handling standard library errors. **Text Book 1: Chapter 10: 10.1,10.2,10.3,10.5,10.7,10.8,10.9,10.10, Chapter 12:12.1-12.4, Chapter 13:13.1-13.3**	**10**

Note 1: All units will have internal choice

Note 2: Three Assignments are evaluated for 10 marks:

Assignment – I from Units 1 and 2.
Assignment – II from Units 3 and 4
Assignment -III from Unit 5

Note 3:Subject Seminar and Group Activity is evaluated for 10 marks

Course Outcomes:

After the completion of the above course students will be able to

CO1: How to respond to security alerts which identifies software issues

CO2: Define methodology for security testing and use appropriate tools in its implementation

CO3: Identify possible security programming errors

CO4: Define methodology for security testing and use appropriate tools in its implementation

COs	**Mapping with POs**
CO1	PO1,PO5,PO6
CO2	PO1,PO2,PO3,PO4,PO6
CO3	PO2,PO4,PO5,PO6
CO4	PO2,PO3,PO6

TEXT BOOKS:

1. Robert C. Seacord, “The CERT ® C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems, Second Edition”, Addison Wesley Professional, April 2014.

2. David Wheeler, “Secure Programming for Linux and Unix HowTo”, Linux Documentation project, Aug 2004.

REFERENCE BOOKS:

1. JohnViega, Matt Messier, “Secure Programming Cookbook for C and C++”, O'Reilly Media, 1st Edition, July 2003.

Course Title : INFORMATION SECURITY POLICIES IN INDUSTRY		
Course Code: 20SCF23	**No. of Credits:3= 3 :0 : 0 (L-T-P)**	**No.of Lecture Hours/Week: 4**
Exam Duration : 3 hours	**CIE + SEE = 50 + 50 =100**	**Total No. of Contact Hours : 52**

Course Objectives:

1. Explain management's responsibilities and role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines
2. Illustrate the differences between the organization's general information security policy and the needs and objectives of the various issue-specific and system-specific policies the organization will create..
3. Know what an information security blueprint is and what its major components are.
4. How an organization institutionalizes its policies, standards, and practices using education, training and awareness programs.
5. Become familiar with what viable information security architecture is, what it includes, and how it is used.

UNIT No	**Syllabus Content**	**No of Hours**
1	Introduction to Information Security Policies: About Policies, why Policies are Important, When policies should be developed, How Policy should be developed, Policy needs, Identify what and from whom it is being protected, Data security consideration, Backups, Archival storage and disposal of data, Intellectual Property rights and Policies, Incident Response and Forensics, Management Responsibilities, Role of Information Security Department, Security Management and Law Enforcement, Security awareness training and support. **[Chap1,2,3]**	**12**
2	Policy Definitions, Standards, Guidelines, Procedures Writing The Security Policies: Physical security; Computer location and Facility construction, Facility access controls, Contingency Planning, General computer systems security, Periodic System and Network Configuration Audits, Staffing Consideration Authentication and Network Security; Network Addressing and Architecture, Access Control, Login Security, Passwords, User Interface, Access Controls, Telecommuting and Remote Access**. [Chap 4,5]**	**8**
3	Writing The Security Policies: Internet Security Policies; Understanding the Door to the Internet, Administrative and User Responsibilities, WWW Policies, Application Responsibilities, VPNs, Extranets, Intranets and other tunnels, Modems and other Backdoors, Employing PKI and other controls, Electronic Commerce. E-mail Security Policies; Rules for using email, Administration of email, Use of email for confidential communication. Viruses ,Worms and Trojan Horses: The need for protection, Establishing Type of Viruses Protection, Rules for handling Third Party Software, User Involvement with Viruses. **[Chap 6,7,8]**	**12**

4	Encryption: Legal Issues, Managing Encryption , Handling Encryption and Encrypted data, Key Generation considerations, Key Management. Software Development policies: Software development processes, Testing and Documentation, Revision control and Configuration management, Third Party Development, Intellectual Property Issues.**[Chap 9,10]**	**8**
5	Maintaining the Policies: Writing the AUP, User Login Responsibilities, Organization's responsibilities and Disclosures, Compliance and Enforcement, Testing and Effectiveness of Policies, Publishing and Notification Requirements of the Policies, Monitoring, Controls and Remedies, Administrator Responsibility, Login Considerations, Reporting of security Problems, Policy Review Process, The Review Committee, Sample Corporate Policies, Sample Security Policies.**[Chap 11,12,13]**	**12**

Note 1: All units will have internal choice
Note 2: Three Assignments are evaluated for 10 marks:
Assignment – I from Units 1 and 2.
Assignment – II from Units 3 and 4
Assignment -III from Unit 5
Note 3:Subject Seminar & Group Activity is evaluated for 10 marks

Course Outcomes:
After the completion of the above course students will be able to

CO1: Explain the content, need, and responsibilities of information security policies..
CO2: Explain the standards, guidelines, Procedures, and key roles of the organization.
CO3:. Able to write policy document for securing network connection and interfaces
CO4: Explain the threats to the stored data or data in transit and able to write policy document.
CO5: Able to write, monitor, and review policy document.

COs	**Mapping with POs**
CO1	PO1,PO2,PO9
CO2	PO2,PO3,PO4,PO9,PO12
CO3	PO2,PO3,PO4,PO9,PO12
CO4	PO2,PO3,PO4,PO9,PO12

TEXT BOOKS:

1. Scott Barman, Writing Information Security Policies, Sams Publishing, 2002.

REFERENCE BOOKS / WEBLINKS:

1. Thomas R Peltier, Justin Peltier, John Backley, "Information Security Fundamentals", Auerbach publications, CRC Press, 2005.
2. Harold F. Tipton and Micki Krause "Information Security Management Handbook", Auerbach publications, 5th Edition, 2005.

Course Title : OPERATING SYSTEM SECURITY		
Course Code: 20SCF24	**No. of Credits:3 = 3 : 0 : 0 (L-T-P)**	**No.of Lecture Hours/Week: 4**
Exam Duration: 3 hours	**CIE + SEE = 50 + 50 =100**	**Total No. of Contact Hours : 52**

Course Objectives:

1. Define fundamental concepts and mechanisms for enforcing security in OS.
2. Build a secure OS by exploring the early work in OS.
3. Illustrate formal security goals and variety of security models proposed for development of secure operating systems.
4. Explain architectures of various secure OS and retrofitting security feature on existing commercial OS's.
5. Analyze variety of approaches applied to the development & extension services for securing operating systems.

UNIT No	Syllabus Content	No of Hours
1	**Introduction**: Secure Os, Security Goals, Trust Model, Threat Model **Access Control Fundamentals**: Protection system Lampson's Access Matrix, Mandatory protection system, Reference Monitor,, Secure OS definition , Assessment Criteria T1: 1.1,1.2,1.3,1.4, 2.1,2.2,2.3,2.4	**10**
2	Multics: Multics History, The multics system: Multics System: Multics Fundamentals, multics security fundamentals , Multics protection system models, multics protection system, Multics reference monitor, multics security, multics vulnerability analysis. T1: 3.1,3.2,3.3,3.4	**10**
3	**Security in ordinary operating system**: UNIX security, Windows security. **Verifiable security goals**: Information flow, information flow secrecy models, information flow integrity models, covert channels. T1:4.1,4,2,4.3,5.1,5.2,5.3,5.4	**10**
4	**Security Kernels**: The Security Kernels, secure communications processor: Scomp architecture , Gemini secure OS. **Securing commercial OS**: Retrofitting security into a commercial OS, History Retrofitting commercial OS, Commercial era, microkernel era, UNIX era T1:6.1,6.2,6.3,7.1,7.2,7.3,7.4,7.5	**10**
5	**Case study: Solaris Extensions Trusted extensions**: Trusted extensions Access control, Solaris compatibility, trusted extensions Mediations, Process rights management, Role based access control, Trusted extensions networking ,Trusted extensions multilevel services, Trusted extensions administration. **Case study: Building secure OS for Linux**: Linux security modules, security enhanced LinuxT1:8.1 to 8.8,9.1,9.2	**12**

Note 1: All units will have internal choice
Note 2: Three Assignments are evaluated for 10 marks:
Assignment – I from Units 1 and 2.
Assignment – II from Units 3 and 4
Assignment -III from Unit 5
Note 3:Subject Seminar & Group Activity is evaluated for 10 marks

Course Outcomes: After the completion of the above course students will be able to
CO1: Gain the knowledge of fundamental concepts and mechanisms for enforcing security in OS.

CO2:. Analyze how to build a secure OS by exploring the early work in OS.

CO3: Identify and compare different formal security goals and variety of security models proposed for development of secure operating systems.

CO4: Interpret architectures of various secure OS and retrofitting security feature on existing commercial OS's

CO5: Analyze variety of approaches applied to the development & extension services for securing operating systems.

COs	**Mapping with POs**
CO1	PO2,PO3,PO5
CO2	PO1, PO2,PO3,PO6,PO7,PO9,PO11
CO3	PO2,PO3, PO5,PO6
CO4	PO2,PO3, PO5,PO6,PO9
CO5	PO2,PO3,PO5,PO6,PO12

TEXT BOOK:
1. Trent Jaeger, Operating system security, Morgan & Claypool Publishers, 2008

REFERENCE BOOKS:

1. Michael Palmer, Guide to Operating system Security Thomson
2. Andrew S Tanenbaum, Modern Operating systems, 3rd Edition
3. Secure Operating Systems. John Mitchell. Multics-Orange Book Claremont.

Google book
https://books.google.co.in/books?id=P4PYPSv8nBMC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

https://www.tutorialspoint.com/unix/unix-file-permission.htm

ELECTIVE-2

Course Title : INTERNET OF THINGS SECURITY		
CourseCode:20SCF251	**No. of Credits:3=3 : 0 : 0 (L-T-P)**	**No. of lecture hours/week : 4**
Exam Duration : **3 hours**	**CIE + SEE = 50 + 50 =100**	**Total No. of Contact Hours :52**

Course Objectives

1. To learn the cyber versus IOT security policy and lifecycle of IOT device.
2. To understand the Security requirements in IOT Architecture
3. To analyze the Cryptographic fundamentals role in the IOT
4. To understand the authentication credentials and access control .
5. To comprehend various types Trust models and Cloud Security

UNIT No	**Syllabus Content**	**No of Hours**
1	**DEFINING THE IOT** - Cybersecurity versus IoT security and cyber-physical systems -Why cross-industry collaboration is vital - IoT uses today - Energy industry and smart grid , Connected vehicles and transportation ,Manufacturing ,Wearables , Implantables and medical devices -The IoT in the enterprise - The things in the IoT -The IoT device lifecycle -The hardware ,Operating systems , IoT communications ,Messaging protocols ,Transport protocols ,Network protocols ,Data link and physical protocols -IoT data collection, storage, and analytics -IoT integration platforms and solutions - The IoT of the future and the need to sec **TEXT BOOK 1:Chapter1-1.1,1.2,1.3,1.4,1.5**	**12**
2	**INTRODUCTION: SECURING THE INTERNET OF THINGS** , Security Requirements in IoT Architecture - Security in Enabling Technologies - Security Concerns in IoT Applications. **Security Architecture in the Internet of Things** - Security Requirements in IoT - Insufficient Authentication/Authorization - Insecure Access Control - Threats to Access Control, Privacy, and Availability - Attacks Specific to IoT. **TEXT BOOK 2: Chapter1- 1.1,1.2,1.3,1.4** **Chapter2:2.1,2.2,2.3,2.4,2.5,2.6**	**10**
3	**CRYPTOGRAPHIC FUNDAMENTALS FOR IOT**-Cryptographic primitives and its role in IoT – Encryption and Decryption – Hashes – Digital Signatures – Random number generation – Cipher suites – key management fundamentals – cryptographic controls built into IoT messaging and communication protocols **TEXT BOOK 1: Chapter5-5.1,5.2,5.3,5.4,5.5**	**10**
4	**IDENTITY & ACCESS MANAGEMENT SOLUTIONS FOR IOT**	

	,Identity lifecycle –authentication credentials – IoT IAM infrastructure – Authorization with Publish / Subscribe schemes – access control witin communication protocols . **TEXT BOOK 1:Chapter 6-6.1,6.2,6.3,6.4,6.5,9.6**	**10**
5	**CLOUD SECURITY FOR IOT**, Cloud services and IoT – offerings related to IoT from cloud service providers – Cloud IoT security controls – An enterpriseIoT cloud security architecture – New directions in cloud enabled IoT computing. **TEXT BOOK 1:Chapter 9-9.1,9.2,9.3,9.4,9.5,9.6,**	**10**

Note 1: All units will have internal choice

Note 2: Three Assignments are evaluated for 10 marks:

Assignment – I from Units 1 and 2.
Assignment – II from Units 3 and 4
Assignment -III from Unit 5

Note 3:Subject Seminar & Group Activity is evaluated for 10 marks

Course outcomes:

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

CO1: Develop security schemes for the applications of IOT in real time scenarios

CO2:Identify different Security requirements in IOT architecture.

CO3:Model the cryptographic primitives and its role

CO4:Understand an identity lifecycle and authentication credentials for IOT

CO5:Understand the trust models and cloud security for IOT

COs	**Mapping with PO's**
CO1	PO3,PO4,PO5,PO6,PO9,PO10
CO2	PO3,PO4,PO5,PO6,PO7,PO9,PO10
CO3	PO4,PO6,PO7,PO8,PO9,PO11
CO4	PO4,PO5,PO8,PO9,PO10,PO11
CO5	PO4,PO5,PO6,PO7,PO9,PO10

TEXT BOOK:

1. Practical Internet of Things Security (Kindle Edition) by Brian Russell, Drew Van Duren
2. Securing the Internet of Things Elsevier

REFERENCE BOOKS/WEBLINKS

1. Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations

Course Title:MOBILE DEVICE FORENSICS		
Course Code:20SCF252	**No. of Credits: 3 = 3:0:0(L-T-P-S)**	**No. of lecture hours/week : 4**
Exam Duration : 3 hours	**CIE + SEE = 50+50=100**	**Total No. of Contact Hours : 52**

Course objectives:

1. Basic Concepts in Mobile Forensics.
2. Mobile Device Data Storage.
3. Identify, preserve, extract, analyze, and report data from mobile devices.
4. Acquiring Evidence from Mobile devices.

Unit No.	Syllabus	No. of Hours
1	**Android and mobile forensics:** Introduction, Android platform, Linux, Open source software and forensics, Android Open Source Project, Internationalization, Android Market, Android forensics Text1:Ch1	**10**
2	**Android hardware platforms:** Overview of core components, Overview of different device types, Read-only memory and boot loaders, Manufacturers, Specific devices. Text1:Ch2	**12**
3	**Android software development kit and android debug bridge:** Android platforms, Software development kit (SDK), Android security model, Forensics and the SDK. Text1:Ch3	**10**
4	**Android file systems and data structures:** Data in the shell, Type of memory, File systems,Mounted file systems and directory structures. Android forensic techniques: Procedures for handling an Android device, Imaging Android USB mass storage devices, Logical techniques, Physical techniques Text1:Ch4	**10**
5	**Android device data and app security:** Data theft targets and attack vectors, Security considerations, Individual security strategies, Corporate security strategies, App development security strategies. Android application and forensic analysis: Analysis techniques, FAT forensic analysis, YAFFS2 forensic analysis, Android app analysis. Text1:Ch5	**10**

Note 1: All units will have internal choice
Note 2: Three Assignments are evaluated for 10 marks:
Assignment – I from Units 1 and 2.
Assignment – II from Units 3 and 4
Assignment -III from Unit 5
Note 3:Subject Seminar and Group Activity is evaluated for 10 marks

Course Outcomes:

At the end of the course, the students will be able to:
CO1:Describe security risks and vulnerabilities from mobile devices and network access.
CO2:Explain the methods and procedures used in forensics investigations.
CO3:Have knowledge of the global security threats and vulnerabilities of mobile devices and networks.
CO4:Carry out a forensics investigation of mobile and network devices..

COs	Mapping with PO's
CO1	PO1,PO4
CO2	PO2,PO3,PO4
CO3	PO3,PO4
CO4	PO3,PO4,PO5,PO6
CO5	PO4,PO8,PO9,PO11

Text Books:

1. Android Forensics Investigation, Analysis, and Mobile security for Google Android, Andrew Hoog, John McCash, Technical Editor, Elsevier, 2011.

Reference Books:

1. Satish Bommisetty, Rohit Tamma, Heather Mahalik "Practical Mobile Forensics", Kindle
Edition, Packt Publishing (21 July 2014).

2. Andrew Martin," Mobile Device Forensics" SANS Institute 2009

Course Title : DATABASE SECURITY		
CourseCode:20SCF253	**No. of Credits:3=3 : 0 : 0 (L-T-P)**	**No. of lecture hours/week : 4**
Exam Duration : **3 hours**	**CIE + SEE = 50 + 50 =100**	**Total No. of Contact Hours :52**

Course Objectives

1. Fundamental security concepts and architectures that serve as building blocks to database security
2. Concepts of user account management and administration, including security risks
3. To use current database management system to design and configure the user and data permissions
4. Operational components necessary to maximize database security using various security models

UNIT No	Syllabus Content	No of Hours
1	Introduction: Introduction to Databases, Security Problems in Databases Security Controls Conclusions. Security Models 1: Introduction, Access Matrix Model, TakeGrant Model, Acten Model, PN Model, Hartson and Hsiao's Model, Fernandez's Model, Bussolati and Martella's Model for Distributed databases.	**12**
2	Security Models 2: Bell and LaPadula's Model, Biba's Model, Dion's Model, Sea View Model, Jajodia and Sandhu's Model, The Lattice Model for the Flow Control conclusion. Security Mechanisms: Introduction, User Identification/Authentication, Memory Protection, Resource Protection, Control Flow Mechanisms, Isolation, Security Functionalities in Some Operating Systems, Trusted Computer System, Evaluation Criteria.	**10**
3	Security Software Design: Introduction, A Methodological Approach to Security, Software Design, Secure Operating System Design, Secure DBMS Design, Security Packages, Database Security Design	**10**
4	Statistical Database Protection & Intrusion Detection Systems: Introduction, Statistics, Concepts and Definitions, Types of Attacks, Inference Controls, evaluation Criteria for Control Comparison, Introduction IDES System, RETISS System, ASES System Discovery	**10**
5	Models For The Protection Of New Generation Database Systems 1: Introduction, A Model for the Protection of Frame Based Systems, A Model for the Protection of Object-Oriented Systems, SORION Model for the Protection of Object-Oriented Databases. Models For The Protection Of New Generation Database Systems 2: A Model for the Protection of New Generation Database Systems, the Orion Model, Jajodia and Kogan's Model, A Model for the Protection of Active Databases Conclusions	**10**

Note 1: All units will have internal choice
Note 2: Three Assignments are evaluated for 10 marks:
Assignment – I from Units 1 and 2.
Assignment – II from Units 3 and 4
Assignment -III from Unit 5
Note 3:Subject Seminar and Group Activity is evaluated for 10 marks

Course outcomes:

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

CO1: Carry out a risk analysis for a large database

CO2:Implement identification and authentication procedures, fine-grained access control and data encryption techniques

CO3:Set up accounts with privileges and roles

CO4:Audit accounts and the database system.

COs	Mapping with PO's
CO1	PO3,PO4,PO5,PO6,PO9,PO10
CO2	PO3,PO4,PO5,PO6,PO7,PO9,PO10
CO3	PO4,PO6,PO7,PO8,PO9,PO11
CO4	PO4,PO5,PO8,PO9,PO10,PO11
CO5	PO4,PO5,PO6,PO7,PO9,PO10

Text Books

1. Database Security and Auditing, Hassan A. Afyoun i, India Edition, CENGAGE Learning, 2009.
2. Database Security, Castano, Second edition, Pearson Education

Reference Books:

1. Database security by Alfred Basta, Melissa Zgola , CENGAGE learning

Course Title : STORAGE MANAGEMENT AND SECURITY		
Course Code: 20SCF254	**No. of Credits:3 = 3 : 0 : 0 (L-T-P)**	**No.of Lecture Hours/Week: 4**
Exam Duration : 3 hours	**CIE + SEE = 50 + 50 =100**	**Total No. of Contact Hours : 52**

Course Objectives:

1. To explain the basic information storage and retrieval concepts.
2. To understand the issues those are specific to efficient information retrieval.
3. To design and implement a small to medium size information storage and Retrieval system.
4. To implement security issues while storing and retrieving information.

UNIT No	**Syllabus Content**	**No of Hours**
1	Storage System- Introduction to Information Storage and Management, Storage System Environment, Data Protection: Raid, Intelligent Storage System.	**10**
2	Storage Networking Technologies and Virtualization, Storage Networks, Network Attached Storage, IP SAN, Content Addressed Storage, Storage Virtualization.	**10**
3	Introduction to Business Continuity, Backup and Recovery, Local Replication, Remote Replication.	**10**
4	Securing the storage Infrastructure, Storage Security Framework, Risk Triad, Storage Security Domains, Security Implementation in Storage Networking.	**10**
5	Managing the Storage Infrastructure, Monitoring the Storage Infrastructure, Storage Management Activities, Developing an Ideal Solution, Concepts in Practice,	**12**

Note 1: All units will have internal choice
Note 2: Three Assignments are evaluated for 10 marks:
Assignment – I from Units 1 and 2.
Assignment – II from Units 3 and 4
Assignment -III from Unit 5
Note 3:Subject Seminar and Group Activity is evaluated for 10 marks

Course Outcomes:
After the completion of the above course students will be able to

CO1 Search, retrieve and synthesize information from a variety of systems and sources
CO2. Evaluate systems and technologies in terms of quality, functionality, cost-effectiveness and adherence to professional standards.
CO3. Integrate emerging technologies into professional practice.
CO4. Apply theory and principles to diverse information contexts.

COs	**Mapping with POs**
CO1	PO1, PO2,PO3,PO5
CO2	PO1, PO2,PO3,PO6,PO7,PO9,PO11
CO3	PO2,PO3, PO5,PO6
CO4	PO2,PO3, PO5,PO6,PO9

TEXT BOOKS:

1. Information Storage and Management: Storing, Managing, and Protecting Digital
   Information, EMC Corporation
2. John Chirillo, Scott Blaul, "Storage Security: Protecting SAN, NAS and DAS", Wiley Publishers, 2003
3. David Alexander, Amanda French, David Sutton," Information Security Management Principles" The British Computer Society, 2008.

Course Title : ETHICAL HACKING LABORATORY		
Course Code: 20SCFL26	**No. of Credits: 2= 0:0:3 (L-T-P)**	**No. of Lecture Hours/Week: 3**
Exam Duration : 3 hours	**Exam Marks: CIE + SEE = 50 + 50 = 100**	

Course Objectives:

1. Evaluate modern tools
2. Analyze packet capturing in network
3. Define forensic analysis
4. Security in various web applications

I. LIST OF PROGRAMS

1. Wireshark: Experiment to monitor live network capturing packets and analyzing over the live Network.

2. LOIC: DoS attack using LOIC.

3. FTK: Bit level forensic analysis of evidential image and reporting the same.

4. Darkcomet : Develop a malware using Remote Access Tool Darkcomet to take a remote access over network. 4.

5. HTTrack: Website mirroring using Httrack and hosting on a local network.

6. XSS: Inject a client side script to a web application.

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

NOTE:

1 . All laboratory experiments (nos) are to be included for practical examination.
2 . Students are allowed to pick one experiment from each part and execute both
3 . Strictly follow the instructions as printed on the cover page of answer script for breakup of mark

Course Outcomes:

After completing the course the students are able to:

CO1: Evaluate modern tools.
CO2: Analyze packet capturing in network.
. **CO3:** Define forensic analysis
CO4: Security in various web applications.

COs	**Mapping with POs**
CO1	PO2,PO3,PO5
CO2	PO2,PO3,PO6,PO9
CO3	PO2,PO3,PO5,PO6
CO4	PO2,PO3,PO5,PO9
CO5	PO2,PO3,PO5,PO6

Course Title : RESEARCH METHODOLOGY		
Course Code Code:18RM27	**No. of Credits :2= 0:1:0(L-T-P)**	**No. of lecture hours/week : 02**
Exam Duration : 3 hours	**CIE +SEE = 50+50 =100**	

Sub. Title :Mini Project/Industry Visit/Field Work		
Sub Code:20SCFL28	**No. of Credits :2= 0:0:6(L-T-P)**	**No. of lecture hours/week : 06**
Exam Duration : 3 hours	**CIE = 50**	

Detailed Scheme

ACADEMIC YEAR 2019-2020

Dr. Ambedkar Institute of Technology
Bangalore

III-IV(2018-2020 BATCH)

M. Tech in Cyber Forensics and Information Security

Department Of Information Science and Engineering

Dr. Ambedkar Institute of Technology

SCHEME OF TEACHING AND EXAMINATION III SEMESTER (Autonomous) 2019-20

M. Tech in **Cyber Forensics and Information Security**

Batch:2018-2020

III semester

o.	Sub Code	Subject Title	Teaching Department	Teaching hours per week			Maximum Marks allotted			Examination Credits
				Lecture	Tutorial/ Seminar/ Assignment	Practical / Field Work	CIE	SEE	Total	
1.	18SCF31	File System Forensic Analysis	ISE	-	-		50	50	100	**4**
2.	18SCF32X	Professional Elective 3	ISE	-	-	-	50	50	100	**3**
3.	18SCF33X	Professional Elective 4	ISE	-	-	-	50	50	100	**3**
4	18SCFI34	Internship					50	50	100	**8**
5	18SCFS35	Technical Seminar					50		50	**2**
6.	18SCFP36	Project phase - I	ISE	-	-	-	50	-	50	**2**
Total							**300**	**200**	**ISE**	**22**

Professional Elective 3			Professional Elective 4		
Sl .No	Name of the Subject	Subject Code	Sl .No	Name of the Subject	Subject Code
1	Block chain technology	18SCF321	1	Cyber Laws and Ethics	18SCF331
2	Managing Big Data	18SCF322	2	Social Network Analysis	18SCF332
3	Artificial Intelligent & Agent Technology	18SCF323	3	Distributed Computing	18SCF333
4	Machine Learning	18SCF324	4	Biometric Security	18SCF334

Note:

1. **Technical Seminar:** CIE marks shall be awarded by a committee comprising of HoD as Chairman, Guide/co-guide, if any, and a senior faculty of the department. Participation in the seminar by all postgraduate students of the same and other semesters of the programme shall be mandatory. The CIE marks awarded for Technical Seminar, shall be based on the evaluation of Seminar Report, Presentation skill and Question and Answer session
2. **Project Phase-1:** Students in consultation with the guide/co-guide if any, shall pursue literature survey and complete the preliminary requirements of selected Project work. Each student shall prepare relevant introductory project document, and present a seminar. CIE marks shall be awarded by a committee comprising of HoD as Chairman, Guide/co-guide if any, and a senior faculty of the department. The CIE marks awarded for project work phase -1, shall be based on the evaluation of Project Report, Project Presentation skill and Question and Answer session
3. SEE as per the norms

4. **2. Internship:** Those, who have not pursued /completed the internship shall be declared as failed and have to complete during subsequent SEE examinations after satisfying the internship requirements. Internship SEE shall be as per the norms.

HEAD DEPT. OF INFORMATION SCIENCE & ENGG

Dr. Ambedkar Institute of Technology

SCHEME OF TEACHING AND EXAMINATION (Autonomous) 2019-20

M. Tech in **Cyber Forensics and Information Security**

Batch:2018-2020

IV semester

Sl. No.	Sub Code	Subject Title	Teaching Department	Teaching hours per week			Maximum Marks allotted			Examination Credits
				Lecture	Tutorial/ Seminar/ Assignment	Practical / Field Work	CIE	SEE	Total	
1	18SCFP41	Project Work Phase II – Midterm Internal Evaluation	…...	-	-	-	50		50	**2**
2	18SCFP42	Project work evaluation and viva voce					100	100	200	**22**
Total							**150**	**100**	**250**	**24**
Grand Total (I to IV Semester) : 88 Credits										

1. Project Phase-2:

CIE marks shall be awarded by a committee comprising of HoD as Chairman, Guide/co-guide, if any, and a Senior faculty of the department. The CIE marks awarded for project work phase -2, shall be based on the evaluation of Project Report subjected to plagiarism check, Project Presentation skill and Question and Answer session in the ratio 50:25:25.

SEE shall be at the end of IV semester. Project work evaluation and Viva-Voce examination (SEE), after satisfying the plagiarism check, shall be as per the norms.

HEAD DEPT. OF INFORMATION SCIENCE & ENGG

III SEMESTER

Sub Title : **FILE SYSTEM FORENSIC ANALYSIS**		
Sub Code: 18SCF31	**No. of Credits:3=4 : 0 : 0 (L-T-P)**	**No.of Lecture Hours/Week: 4**
Exam Duration : 3 hours	**CIE + SEE = 50 + 50 =100**	**Total No. of Contact Hours : 52**

Course Objectives:

1. Computer file system and storage analysis
2. Basics of Computer forensics
3. Role of forensics in business world.

UNIT No	Syllabus Content	No of Hours
1	Volume Analysis: Introduction, Background, Analysis Basics, Summary. PC-based Partitions: DOS Partitions, Analysis Considerations, Apple Partitions, Removable Media. Server-based Partitions: BSD Partitions, Sun Solaris Slices, GPT Partitions, Multiple Disk Volumes: RAID, Disk Spanning. Chapter 4, 5,6,7	**10**
2	File System Analysis: What Is a File System?, File System Category, Content Category, Metadata Category, File Name Category, Application Category, Application-level Search Techniques, Specific File Systems FAT Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, The Big Picture, Other Topics. FAT Data Structures: Boot Sector, FAT32 FSINFO, FAT, Directory Entries, Long File Name Directory Entries, Chapter 8,9,10	**10**
3	NTFS Concepts: Introduction, Everything is a File, MFT Concepts, MFT Entry Attribute Concepts, Other Attribute Concepts, Indexes, Analysis Tools. NTFS Analysis: File System Category, Content Category, Metadata Category, File Name Category, Application Category, The Big Picture. NTFS Data Structures: Basic Concepts, Standard File Attributes, Index Attributes and Data Structures, File System and Meta Data Files. Chapter 11,12,13	**10**
4	Ext2 and Ext3 Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, Application Category. The Big Picture. Ext2 and Ext3 Data Structures: Superblock, Group Descriptor Tables, Block Bitmap, Inodes, Extended Attributes, Directory Entry, Symbolic Link, Hash Trees, Journal Data Structures, Chapter 14,15	**10**

5	UFS1 and UFS2 Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, The Big Picture. UFS1 and UFS2 Data Structures: UFS1 Superblock, UFS2 Superblock, Cylinder Group Summary, UFS1 Group Descriptor, UFS2 Group Descriptor, Block and Fragment Bitmaps, UFS1 Inodes, UFS2 Inodes, UFS2 Extended Attributes, Directory Entries Chapter 17	**12**

Note 1: All units will have internal choice
Note 2: Three Assignments are evaluated for 10 marks:
Assignment – I from Units 1 and 2.
Assignment – II from Units 3 and 4
Assignment -III from Unit 5
Note 3:Subject Seminar is evaluated for 10 marks

Course Outcomes:
After the completion of the above course students will be able to

CO1: Compare the different file systems for storing information

CO2:. Illustrate the role of computer forensics in the business and private world

CO3: Illustrate the role of computer forensics in the business and private world

.**CO4:** Identify some of the current techniques and tools for forensic examinations

COs	**Mapping with POs**
CO1	PO2,PO3,PO5
CO2	PO1, PO2,PO3,PO6,PO7,PO9,PO11
CO3	PO2,PO3, PO5,PO6
CO4	PO2,PO3, PO5,PO6,PO9
CO5	PO2,PO3,PO5,PO6,PO12

TEXT BOOK:

1. Brian Carrier, File System Forensic Analysis, Pearson Education, 2005

REFERENCE BOOKS:

1. Machtelt Garrels, “Introduction to Linux A Hands-On Guide”, Third Edition, Fultus Corporation Publisher, 2010.

Professional Elective 3

Sub Title : **BLOCKCHAIN TECHNOLOGY**		
Sub Code: 18SCF321	**No. of Credits:3=4 : 0 : 0 (L-T-P)**	**No.of Lecture Hours/Week: 4**
Exam Duration : 3 hours	**CIE + SEE = 50 + 50 =100**	**Total No. of Contact Hours : 52**

Course Objectives:

- To understand the function of Blockchains as a method of securing distributed ledgers, consensus on their contents.
- To learn blockchain operations as distributed data structures and decision making systems
- To gain knowledge of Bitcoin transaction, mining etc.,
- To understand applications of BlockChain Technology.

UNIT No	**Syllabus Content**	**No of Hours**
1	**Introduction:** Block Header – Block Identifiers – The Genesis Block – Linking Blocks in the Blockchain – Merkle Trees – What is Bitcoin? – History of Bitcoin – Bitcoin Uses, Users, and their Stories	**10**
2	**Mining and Consensus:** De-centralized Consensus – Independent Verification of Transactions – Mining Nodes – Aggregating Transactions into Blocks – Constructing the Block Header – Mining the Block – Validating a new Block – Assembling and selecting Chains of Blocks – Mining and the Hashing Race	**10**
3	**Contracts:** Financial Services – Crowdfunding – Smart Property – Smart Contracts – Blockchain Development Platforms – Blockchain Ecosystem – Ethereum	**10**
4	**Bitcoin:** Bitcoin Transactions – Constructing a Transaction – Bitcoin Mining – Keys – Public keys and Private Keys – Bitcoin Addresses – Wallets – Advanced Keys and Addresses – Transaction Lifecycle – Transaction Outputs and Inputs – Transaction Scripts and Scripting Language	**10**
5	**Applications:** Namecoin: Decentralized Domain Name System – Digital Identity Verification – Digital Art – Blockchain Government – Blockchain Science – Blockchain Health – Blockchain Learning – Bitcoin Security	**12**

Note 1: All units will have internal choice
Note 2: Three Assignments are evaluated for 10 marks:
Assignment – I from Units 1 and 2.
Assignment – II from Units 3 and 4
Assignment -III from Unit 5
Note 3:Subject Seminar is evaluated for 10 marks

Course Outcomes:
After the completion of the above course students will be able to

CO1: Analyze the importance of structure of a blockchain and why/when it is better than a simple distributed database.

CO2: Analyze the process of consensus and mining algorithms.

CO3: Use the smart contract platforms.

CO4: Design different use cases of blockchain technology.

COs	**Mapping with POs**
CO1	PO2,PO6
CO2	PO2,PO3,PO6
CO3	PO2,PO5,PO6
CO4	PO2,PO3,PO6

Textbooks:

1. Mastering Bitcoin: Unlocking Digital Crypto-Currencies, by Andreas Antonopoulos, O'Reilly Media, 2014
2. Blockchain: Blueprint for a New Economy, by Melaine Swan, O'Reilly Media, 2015

References:

1. Hyperledger Fabric – https://www.hyperledger.org/projects/fabric
2. Zero to Blockchain – An IBM Redbooks course, by Bob Dill, David Smits – https://www.redbooks.ibm.com/Redbooks.nsf/RedbookAbstracts/crse0401.html

MANAGING BIG DATA		
Sub Code: 18SCF322	**No. of Credits:3=4 : 0 : 0 (L-T-P)**	**No.of Lecture Hours/Week: 4**
Exam Duration : 3 hours	**CIE + SEE = 50 + 50 =100**	**Total No. of Contact Hours : 52**

Course Objectives:

- Define big data for business intelligence.
- Analyze business case studies for big data analytics.
- Explain managing of Big data Without SQL.
- Develop map-reduce analytics using Hadoop and related tools

UNIT No	Syllabus Content	No of Hours
1	**INTRODUCTION TO BIG DATA :**Introduction– distributed file system– Big Data and its importance, Four Vs, Drivers for Big data, Big data analytics, Big data applications. Algorithms using map reduce. Text1:Ch1,Ch2	10
2	**INTRODUCTION TO HADOOP AND HADOOP ARCHITECTURE:**Big Data – Apache Hadoop & Hadoop EcoSystem, Moving Data in and out of Hadoop – Understanding inputs and outputs of MapReduce -, Data Serialization. Text1:Ch3,Ch4	10
3	**HDFS, HIVE AND HIVEQL, HBASE:HDFS**-Overview, Installation and Shell, Java API; Hive Architecture and Installation, Comparison with Traditional Database, HiveQL Querying Data, Sorting And Aggregating, Map Reduce Scripts, Joins & Sub queries, HBase concepts, Advanced Usage, Schema Design, Advance Indexing, PIG, Zookeeper , how it helps in monitoring a cluster, HBase uses Zookeeper and how to Build Applications with Zookeeper. Text1:Ch5,Ch6	10
4	**SPARK:**Introduction to Data Analysis with Spark, Downloading Spark and Getting Started, Programming with RDDs, Machine Learning with MLlib.**NoSQL**:What is it?, Where It is Used Types of NoSQL databases, Why NoSQL?, Advantages of NoSQL, Use of NoSQL in Industry, SQL vs NoSQL, NewSQL Text1:Ch7,Ch8	10
5	**Introduction to MongoDB**: key features, Core Server tools, MongoDB through the JavaScript's Shell, Creating and Querying through Indexes, Document-Oriented, principles of schema design, Constructing queries on Databases, collections and Documents , MongoDB Query Language. Text1:Ch9,Ch10	12

Note 1: All units will have internal choice
Note 2: Three Assignments are evaluated for 10 marks:
Assignment – I from Units 1 and 2.
Assignment – II from Units 3 and 4
Assignment -III from Unit 5
Note 3:Subject Seminar is evaluated for 10 marks

Course Outcomes:
After the completion of the above course students will be able to

CO1: Describe Big data and use cases from selected industry domains.

CO2: Discuss about NoSQL Big data management**.**

CO3: Install, configure, and run Hadoop.

CO4: Perform Mapreduce analytics using Hadoop.

CO5: Use Hadoop related tools such as HBase, Cassandra, Pig and Hive for Big Data Analytics..

COs	**Mapping with POs**
CO1	PO2, PO8
CO2	PO4,PO5, PO8
CO3	PO3, PO4, PO5
CO4	PO4, PO5

Textbooks:

1. Tom White, "Hadoop: The Definitive Guide", Third Edition, O'Reilley, 2012.
2. Eric Sammer, "Hadoop Operations", O'Reilley, 2012.

References:

1. VigneshPrajapati, Big data analytics with R and Hadoop, SPD 2013.
2. E. Capriolo, D. Wampler, and J. Rutherglen, "Programming Hive", O'Reilley, 2012.
3. Lars George, "HBase: The Definitive Guide", O'Reilley, 2011.
4. Alan Gates, "Programming Pig", O'Reilley, 2011

ARTIFICIAL INTELLIGENT & AGENT TECHNOLOGY		
Sub Code: 18SCF323	**No. of Credits:3=4 : 0 : 0 (L-T-P)**	**No.of Lecture Hours/Week: 4**
Exam Duration : 3 hours	**CIE + SEE = 50 + 50 =100**	**Total No. of Contact Hours : 52**

Course Objectives:

(1) To Apply a given AI technique to a given concrete problem

(2) To Implement non-trivial AI techniques in a relatively large system

(3) To understand uncertainty and Problem solving techniques.

(4) To understand various symbolic knowledge representation to specify domains and reasoning tasks of a situated software agent.

(5) To understand different logical systems for inference over formal domain representations, and trace how a particular inference algorithm works on a given problem specification.

(6) To understand how to write a Prolog Programs for Artificial Intelligence

Unit No	Syllabus Content	No Of Hours
1	What is Artificial Intelligence: The AI Problems, The Underlying assumption, What is an AI Technique?, The Level of the model, Criteria for success, some general references, One final word and beyond. Problems, problem spaces, and search**:** Defining, the problem as a state space search, Production systems, Problem characteristics, Production system characteristics, Issues in the design of search programs, Additional Problems.Intelligent Agents: Agents and Environments, The nature of environments, The structure of agents. (Text Book 1: Chapter 1 & 2 Text Book 2: Chapter 2)	**10**
2	Heuristic search techniques: Generate-and-test, Hill climbing, Best-first search, Problem reduction, Constraint satisfaction, Mean-ends analysis, Knowledge representation issues**:** Representations and mappings, Approaches to knowledge representation, Issues in knowledge representation, The frame problem. Using predicate logic: Representing simple facts in logic, representing instance and ISA relationships, Computable functions and predicates, Resolution, Natural Deduction. Logical Agents: Knowledge –based agents, the Wumpus world, Logic-Propositional logic, Propositional theorem proving, Effective propositional model checking, Agents based on propositional logic. (Text Book 1: Chapter 3, 4 & 5 Text Book 2: Chapter 6 **)**	**10**
3	Symbolic Reasoning Under Uncertainty: Introduction to nonmonotonic reasoning, Logic for nonmonotonic reasoning, Implementation Issues, Augmenting a problem-solver, Implementation: Depth-first search, Implementation: Breadth-first search. Statistical Reasoning: Probability and bayes Theorem, Certainty factors and rule-based systems, Bayesian Networks(Text Book1: Chaoter 7 & 8 Text Book 2: chapter13)	**10**
4	An Overview of Prolog, An example program: defining family relations Extending the example program by rules, A recursive rule definition, How Prolog answers questions, Declarative and procedural meaning of programs Syntax and Meaning of Prolog Programs, Data objects, Matching	**11**

	Declarative meaning of Prolog programs, Procedural meaning Example: monkey and banana Order of clauses and goals Remarks on the relation between Prolog and logic (Text Book3 : Chapter 1 & 2)	
5	List Operators, Arithmatic, Represenation of lists, some operations on lists, Operator notation, Arithmatic, Using structures: Example programs, Retrieving Structured information from a database, Doing Data abstraction, Simulating a non-deterministic automation, Travel Planning, The Eight queens problems, Controlling, Backtracking, preventing backtracking, Examples Using Cut, Negation as failure, Problems with Cut and negation, Input and Output, communication with file (Text Book 3: Chapter 3, 4, 5 & 6)	**11**

Note 1: All units will have internal choice

Note 2: Three Assignments are evaluated for 10 marks:

Assignment – I from Units 1 and 2.

Assignment – II from Units 3 and 4

Assignment -III from Unit 5

Note 3:Subject Seminar is evaluated for 10 marks

COURSE OUTCOMES:

CO1: Design intelligent agents for problem solving, reasoning, planning, decision making, and learning. specific design and performance constraints, and when needed, design variants of existing algorithms.

CO2: Apply AI technique on current applications.

CO3: Problem solving, knowledge representation, reasoning, and learning.

CO4: Demonstrating how to write programs for Artificial Intelligence

CO5: Solving recursive programs in Prolog

CO6: Analyzing and solving Artificial Intelligence programs by using backtracking methods

CO's	**Mapping with POs**
CO1	PO1, PO2, PO5, PO9
CO2	PO1, PO5, PO11, PO12
CO3	PO1, PO2, PO7, PO9
CO4	PO1, PO2, PO9, PO11
CO5	PO1, PO2, PO11, PO12
CO6	PO1, PO2, PO5, PO11, PO12

Text Books.

(1) Elaine Rich,Kevin Knight, Shivashanka B Nair:Artificial Intelligence, Tata CGraw Hill 3rd edition. 2013, ISBN 10: 0070087709 ISBN 13: 9780070087705

(2) Stuart Russel, Peter Norvig: Artificial Intelligence A Modern Approach, Pearson 3rd edition 2013, ISBN 0-13-604259-7

(3) **Ivan Bratko, PROLOG Programming for Artificial Intelligence**
Published by Pearson Education (US), 2011 ISBN 10: 0321417461 / ISBN 13: 9780321417466

Reference Books:

1. Nils J. Nilsson: “Principles of Artificial Intelligence”, Elsevier, ISBN-13: 9780934613101

Course Title : MACHINE LEARNING		
Course Code: 18SCF324	No. of Credits: 3 =4:0:0:0(L-T-P-S)	No. of lecture hours/week : 4
Exam Duration : 3 hours	CIE + SEE = 50+50=100	Total No. of Contact Hours : 52

Course objectives:

1. To understand the basic concepts of machine learning along with decision trees.
2. To understand the neural networks and genetic algorithms
3. To understand the Bayesian techniques
4. To understand the instant based learning
5. To understand the analytical learning and reinforced learning

Unit No.	Syllabus	No. of Hours
1	**INTRODUCTION and DECISION TREES**: **Machine learning basics:** What is machine learning? Key terminology , Key tasks of machine learning,How to choose the right algorithm, Steps in developing a machine learning application , Why Python. **Classifying with k-Nearest Neighbors** Classifying with distance measurements, Prepare: importing data with Python , Putting the kNN classification, algorithm into action, How to test a classifier, Example: improving matches with kNN, Prepare: parsing data from a text file, Analyze: creating scatter plots with Matplotli, Prepare: normalizing numeric values, Test: testing the classifier as a whole program, Use: putting together a useful system, Example: a handwriting recognition system, Prepare: converting images	11
2	**NEURAL NETWORKS and GENETIC ALGORITHMS:** Biological Multilayer Networks and Back Propagation Algorithms, Genetic Algorithms, Neural Network Representation, Problems, Perceptrons,	10
3	**BAYESIAN AND COMPUTATIONAL LEARNING** Bayes Theorem – Concept Learning – Maximum Likelihood – Minimum Description Length Principle – Bayes Optimal Classifier – Gibbs Algorithm – Naïve Bayes Classifier – Bayesian Belief Network – EM Algorithm – Probably Learning – Sample Complexity for Finite and Infinite Hypothesis Spaces – Mistake Bound Model.	10
4	**K- Nearest Neighbor Learning** – Locally Weighted Regression – Radial Basis Functions – Case-Based Reasoning – Sequential Covering Algorithms – Learning Rule Sets – Learning First Order Rules – Learning Sets of First Order Rules – Induction as Inverted Deduction – Inverting Resolution	10
5	**MODULE V ANALYTICAL LEARNING AND REINFORCED LEARNING** Perfect Domain Theories – Explanation Based Learning – Inductive-Analytical Approaches - FOCL Algorithm – Reinforcement Learning – Task – Q-Learning – Temporal Difference Learning	11

Note 1: All units will have internal choice
Note 2: Three Assignments are evaluated for 10 marks:
Assignment – I from Units 1 and 2.
Assignment – II from Units 3 and 4
Assignment -III from Unit 5
Note 3:Subject Seminar is evaluated for 10 marks

Course Outcomes:

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

CO1: Choose the learning techniques with this basic knowledge. Also, obtain knowledge on decision tree learning.
CO2: Apply andcomprehend neural network and genetic algorithms techniques.
CO3: Obtain knowledge about supervised and semi-supervised learning.
CO4: Differentiate between reinforcement and analytical learning techniques.
CO5: Differentiate different machine learning applications.

COs	**Mapping with PO's**
CO1	PO1,PO4
CO2	PO2,PO3,PO4
CO3	PO3,PO4
CO4	PO3,PO4,PO5,PO6
CO5	PO4,PO8,PO9,PO11

Text Books:

1. Peter Harrington , "Machine Learning in Action", MANNING Shelter Island Publication, ISBN 9781617290183, 2012. Unit1: Chapter 1-2.4 (page no 1 to 36)

2. Tom M. Mitchell, "Machine Learning", McGraw-Hill Education, 2013.
Unit2, Unit3, Unit4 and Unit5: Chapter 4 to chapter 8 (Page no: 81 to 247)

Reference Books:

1. Ethem Alpaydin, "Introduction to Machine Learning", 2nd Ed., PHI Learning Pvt. Ltd., 2013.
2. T. Hastie, R. Tibshirani, J. H. Friedman, "The Elements of Statistical Learning", Springer; 1st edition, 2001.

Professional Elective - 4

Sub. Title : CYBER LAWS AND ETHICS		
Sub. Code:18SCF331	**No. of Credits: 3 =4:0:0(L-T-P-S)**	**No. of lecture hours/week : 4**
Exam Duration : 3 hours	**CIE + SEE = 50+50=100**	**Total No. of Contact Hours : 52**

Course Objectives

- Explain the Indian legal system, ITA 2000/2008, cyber security and related legal issues.
- Explain the Types of contract law, Digital signature and related legal issues, the Intellectual property rights, types of cyber properties, copyright law, patent and related legal issues, the types of cyber crimes and related legal issues
- Explain cyber crime investigation and prosecution in depth.

Unit No.	Syllabus	No. of Hours
1	**Legal Aspects of Information Security:** Basic concepts of Law and Information Security, Overview of Information Security Obligations under ITA 2008, Privacy and Data Protection concepts. **Volume 1: 35-212**	**10**
2	**Cyber Contracts:** Law of contracts applicable for Cyber Space Transactions, Legal Recognition of Electronic Documents, Authentication of Electronic Documents, Types of Cyber space Contracts, Resolution of Disputes in Digital Space, Stamping of Contractual Document. **Volume 2: 219-294**	**10**
3	**Intellectual Property Rights in Cyber Space:** Concept of Virtual Assets, An overview of Intellectual Property Rights, Trademarks and Domain Names, Copyright Law, Law of Patents. **Volume 3: 299-427**	**10**
4	**Cyber Crimes:** Law of Cyber Crimes, Types of Cyber Crimes, Provisions of Cyber Crimes under ITA 2008, System Adjudication, Case Studies. **Volume 4: 434-777**	**10**
5	**Miscellaneous Issues:** Miscellaneous Issues, Evidentiary Issues, Jurisdiction Issues, Information Security Management in corporate Sector. **Volume 5: 785-1041**	**12**

Course Outcomes:

At the end of the course, the students will be able to:
CO1: Describe the Indian legal system, ITA 2000/2008, cyber security and related legal issues.
CO2: Classify the Types of contract law, Digital signature , related legal issues, the Intellectual
property rights, types of cyber properties, copyright law, patent and related legal issues, the types of cyber crimes and related legal issues, the types of cyber crimes and related legal issues.
CO3: Interpret the cyber crime investigation and prosecution in depth.

Note 1: All units will have internal choice
Note 2: Three Assignments are evaluated for 10 marks:
Assignment – I from Units 1 and 2.
Assignment – II from Units 3 and 4
Assignment -III from Unit 5
Note 3:Subject Seminar is evaluated for 10 marks

Cos	**Mapping with PO's**
CO1	PO1,PO2,PO3,PO5
CO2	PO2,PO4,PO5,PO6,PO7
CO3	PO1,PO2,PO3,PO4,PO5,PO6,PO7
CO4	PO1,PO2,PO5,PO7,PO8
CO5	PO1,PO2,PO3,PO9,PO11

Text Books:

1. Cyber Laws for Engineers, Naavi, Ujvala Consultants Pvt Ltd, 2010.

Reference Books:

1. Deborah G Johnson, Computer Ethics, Pearson Education Pub., ISBN : 81-7758-593-2.
2. Earnest A. Kallman, J.P Grillo, Ethical Decision making and Information Technology: An Introduction with Cases, McGraw Hill Pub.
3. John W. Rittinghouse, William M. Hancock, Cyber security Operations Handbook, Elsevier Pub.
4. Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, 2nd Edition, Cengage Learning Pub.
5. Randy Weaver, Dawn Weaver, Network Infrastructure Security, Cengage Learning Pub

SOCIAL NETWORK ANALYSIS		
Course Code:18SCF332	**No. of Credits: 3 =4:0:0:0(L-T-P-S)**	**No. of lecture hours/week : 4**
Exam Duration : 3 hours	**CIE + SEE = 50+50=100**	**Total No. of Contact Hours : 52**

Course objectives:

- List basic principles behind network analysis algorithms.
- Acquire essential knowledge of network analysis.
- Apply real world data with examples from today’s most popular social networks.
- Plan and execute network analytical computations

Unit No.	Syllabus	No. of Hours
1	**Introduction to social network analysis and Descriptive network analysis:** Introduction to new science of networks. Networks examples. Graph theory basics. Statistical network properties. Degree distribution, clustering coefficient. Frequent patterns. Network motifs. Cliques and k-cores. Text1:Ch1,Ch2	10
2	**Network structure, Node centralities and ranking on network:** Nodes and edges, network diameter and average path length. Node centrality metrics: degree, closeness and betweenness centrality. Eigenvector centrality and PageRank. Algorithm HITS. Text1:Ch3,Ch4	12
3	**Network communities and Affiliation networks:** Networks communities. Graph partitioning and cut metrics. Edge betweenness. Modularity clustering. Affiliation network and bipartite graphs. 1-mode projections. Recommendation systems. Text1:Ch5,Ch6	10
4	**Information and influence propagation on networks and Network visualization:** Social Diffusion. Basic cascade model. Influence maximization. Most influential nodes in network. Network visualization and graph layouts. Graph sampling. Low -dimensional projections. Text1:Ch7,Ch8	10
5	**Social media mining and SNA in real world: FB/VK and Twitter analysis:** Natural language processing and sentiment mining. Properties of large social networks: friends, connections, likes, re-tweets. Text1:Ch9,Ch10	10

Note 1: All units will have internal choice

Note 2: Three Assignments are evaluated for 10 marks:

Assignment – I from Units 1 and 2.

Assignment – II from Units 3 and 4

Assignment -III from Unit 5

Note 3:Subject Seminar is evaluated for 10 marks

Course Outcomes:

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

CO1:Define notation and terminology used in network science.

CO2:Demonstrate, summarize and compare networks.

CO3:Explain basic principles behind network analysis algorithms.

CO4:Analyzing real world network

.

COs	Mapping with PO's
CO1	PO1,PO4
CO2	PO2,PO3,PO4
CO3	PO3,PO4
CO4	PO3,PO4,PO5,PO6
CO5	PO4,PO8,PO9,PO11

Text Books:

1. David Easley and John Kleinberg. "Networks, Crowds, and Markets: Reasoning About a Highly Connected World." Cambridge University Press 2010

Reference Books:

1. Stanley Wasserman and Katherine Faust. "Social Network Analysis. Methods and Applications." Cambridge University Press, 1994.
2. Eric Kolaczyk, Gabor Csardi. “Statistical Analysis of Network Data with R (Use R!)”. Springer,2014.

Course Title: DISTRIBUTED COMPUTING		
Course code: 18SCF333	**No. of Credits:3=4 : 0 : 0 (L-T-P)**	**No. of lecture hours/week : 4**
Exam Duration : 3 hours	**CIE + SEE = 50 + 50 =100**	**Total No. of Contact Hours :52**

Course Objectives

- To learn Concepts of Distributed system Management.
- To acquire knowledge on File Sharing, DFS Implementation, Replication in Distributed File System
- To understand the concepts of Cryptanalysis, Secure channels, Access control
- Overview of security concepts in distributed computing.

UNIT No	Syllabus Content	No of Hours
1	Distributed System management: Introduction, Resource management, Task Assignment Approach, Load Balancing Approach, Load-Sharing Approach, Process management in a Distributed Environment, Process Migration, Threads, Fault Tolerance. TEXT1 Chapter 7	**10**
2	Distributed Shared Memory :Introduction, Basic Concepts of DSM, Hardware DSM, Design Issue in DSM Systems, Issue in Implementing DSM Systems, Heterogeneous and Other DSM Systems, Case Studies TEXT 1 Chapter 8	**10**
3	Distributed File System: Introduction to DFS, File Models, Distributed File System Design, Semantics of File Sharing, DFS Implementation, File Caching in DFS, Replication in DFS, Case studies. Naming: Introduction, Desirable features of a good naming system, Basic concepts, System-oriented names, Object-locating mechanisms, Issues in designing human-oriented names, Name caches, Naming and security, Case study: Domain name service. TEXT 1 Chapter 9,10	**10**
4	Security in distributed systems: Introduction, Cryptography, Secure channels, Access control, Security Management, Case studies. TEXT 1 Chapter 11	**8**
5	Real-Time Distributed operating Systems: Introduction, Design issues in real-time distributed systems, Real-time communication, Real-time scheduling, Emerging Trends in distributed Computing: Introduction to emerging trends, Grid Computing, SOA, Cloud computing, the future of emerging Trends. TEXT 1 Chapter 12 14	**12**

Note 1: All units will have internal choice
Note 2: Three Assignments are evaluated for 10 marks:
Assignment – I from Units 1 and 2.
Assignment – II from Units 3 and 4
Assignment -III from Unit 5
Note 3:Subject Seminar is evaluated for 10 marks

Course Outcomes:
After completing the course the students are able to:.
CO1: Identify the components of Distributed System management
CO2: Realize shared memory concept
CO3 : Apply the concepts of Distributed File System
CO4: Analyze the naming system
CO5: Incorporate the security features in Distributing System Management

Cos	**Mapping with PO's**
CO1	PO2,PO3
CO2	PO2,PO3
CO3	PO2,PO3,PO5
CO4	PO4
CO5	PO2,PO3

TEXT BOOK:

1. Sunitha Mahajan, Seema Shah: Distributing Computing, Published by Oxford University press 2010.

REFERENCE BOOKS/WEBLINKS:

1. Tanenbaum S. Maarten V.S.: Distributed Systems Principles and Paradigms, (Pearson Education)

Course Title : BIOMETRIC SECURITY		
CourseCode:18SCF334	No. of Credits:3=4 : 0 : 0 (L-T-P)	No. of lecture hours/week : 4
Exam Duration : 3 hours	CIE + SEE = 50 + 50 =100	Total No. of Contact Hours :52

Course Objectives

1. Explain the principles used in biometrics algorithms and systems and most important biometric approaches.
2. Illustrate the capability to select a suitable algorithm / system for a given application context (e.g. physical access control)
3. Demonstrate a good understanding of the complex relationships between biometric systems and environmental conditions (e.g. illumination, pose variations etc.) and their impact on biometric performance.
4. Illustrate of data privacy principles and the impact on the design and configuration of biometric systems.

UNIT No	Syllabus Content	No of Hours
1	Biometrics: Introduction, benefits of biometrics over traditional authentication systems, benefits of biometrics in identification systems, selecting a biometric for a system, Applications, Key biometric terms and processes, biometric matching methods, Accuracy inbiometric systems.	12
2	Physiological Biometric Technologies: Fingerprints: Technical description, characteristics, Competing technologies, strengths, weaknesses, deployment. Facial scan: Technical description, characteristics, weaknesses, deployment. Iris scan: Technical description, characteristics, strengths, weaknesses, deployment. Retina vascular pattern: Technical description, characteristics, strengths, weaknesses, deployment. Hand scan: Technical description, characteristics, strengths, weaknesses, deployment , DNA biometrics	10
3	Behavioral Biometric Technologies: Handprint Biometrics, DNA Biometrics, signature and handwriting technology, Technical description, classification, keyboard / keystroke Dynamics, Voice, data acquisition, feature extraction, characteristics, strengths, weaknesses deployment.	10
4	Multi biometrics: Multi biometrics and multi factor biometrics, two-factor authentication with passwords, tickets and tokens, executive decision, implementation plan.	10
5	Case studies on Physiological, Behavioral and multifactor biometrics in identification systems	10

Note 1: All units will have internal choice
Note 2: Three Assignments are evaluated for 10 marks:
Assignment – I from Units 1 and 2.
Assignment – II from Units 3 and 4
Assignment -III from Unit 5

Note 3:Subject Seminar is evaluated for 10 marks

Course outcomes:
Upon completion of the course, the students will be able to
CO1: Visualize traditional and biometric systems.
CO2:Analyze different algorithms of biometric systems.
CO3:Compare strengths and weaknesses of different biometric systems.
CO4: Design different biometric system. • Design multimodal biometric systems.

COs	Mapping with PO's
CO1	PO3,PO4,PO5,PO6,PO9,PO10
CO2	PO3,PO4,PO5,PO6,PO7,PO9,PO10
CO3	PO4,PO6,PO7,PO8,PO9,PO11
CO4	PO4,PO5,PO8,PO9,PO10,PO11
CO5	PO4,PO5,PO6,PO7,PO9,PO10

Text Books

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi, Biometrics –Identity verification in a networked World, Wiley Eastern, 2002.

2. John Chirillo and Scott Blaul, Implementing Biometric Security, Wiley Eastern Publications, 2005. REFERENCE BOOKS/WEBLINKS

Reference Books:

1. John Berger, Biometrics for Network Security, Prentice Hall, 2004.