III B.Tech. CSE (Cyber Security)

I Semester Course Structure

Regulations: R22(CBCS) Admission to I B.Tech : 2022-23 With effect from 2024-25 Onwards

Sl. No.	Course Code	Courses	Category	Periods per Week		Credits	Scheme of Examination Maximum Marks			Pg. No.
				L	T/P/D		CIE (Continuous Internal Evaluation)	SEE (Semester End Examination)	Total	
1	22CY301	Foundations of Cryptography	PC	3	0	3	40	60	100	5
2	22CY302	Malware Analysis and Detection	PC	3	0	3	40	60	100	7
3	22IT301	Web Technologies	PC	3	0	3	40	60	100	8
4	22CY303	IoT and Security Services	PC	3	0	3	40	60	100	10
5	22CS309 /354	Automata Theory and Compiler Design	PC	3	0	3	40	60	100	12
Practical's										
6	22IT331	Web Technologies Lab	PC	0	3	1.5	40	60	100	14
7	22CY331	Cryptography and Compiler Design Lab	PC	0	3	1.5	40	60	100	16
8	22CY332	IoT and Security Services Lab	PC	0	2	1	40	60	100	17
9	22CY333	Advanced Web Programming Lab	PC	0	2	1	40	60	100	18
			Total	**15**	**10**	**20**	**360**	**540**	**900**	
10	22HS302 /352/253	Intellectual Property Rights	MC	3	0	0	100	0	100	20
			Total Hours	**28**						

Service courses of III year I sem

Sl. No.	Course Code	Courses	Branch	Category	Periods per Week		Credits	Scheme of Examination Maximum Marks		
					L	T/P/D		Internal	External	Total
1	22CY333	Advanced Web Programming Lab	**CSE (AI&ML), CSE(DS)**	**PC**	**0**	**2**	**1**	**40**	**60**	**100**

Note: Lecture Hours (L), Tutorials (T), Practicals (P), Drawing (D)

HS: HUMANITIES AND SOCIAL SCIENCES
ES: ENGINEERING SCIENCES
PC: PROFESSIONAL CORE

PE: PROFESSIONAL ELECTIVE
BS: BASIC SCIENCES
MC: MANDATORY COURSE

III B.Tech. CSE (Cyber Security)

II Semester Course Structure

Regulations: R22(CBCS) Admission to I B.Tech : 2022-23 With effect from 2024-25 Onwards

S. No.	Course Code	Courses	Category	Periods per Week		Credits	Scheme of Examination Maximum Marks			Pg. No.
				L	T/P /D		CIE (Continuous Internal Evaluation)	SEE (Semester End Examination)	Total	
1	22CY351	Cryptography and Network Security	PC	3	0	3	40	60	100	21
2	22CY352	Vulnerability Assesment and Penetration Testing	PC	3	0	3	40	60	100	23
3	22CY353	Cyber Crime Investigation and Digital Forensics	PC	3	0	3	40	60	100	25
4	22HS351/301/ 401	Business Economics and Financial Analysis	HS	3	0	3	40	60	100	26
5	**Professional Elective - I:**									
	22DT354	Data Warehousing and Business Intelligence	PE	3	0	3	40	60	100	28
	22CY354	Wireless Networks and Mobile Computing								30
	22AM357	Fundamentals of Artificial Intelligence and Data Science								31
	22CY355	Digital Watermarking and Stegnography								33
Practicals										
6	22CY381	Cyber Crime Investigation and Digital Forensics Lab	PC	0	2	1	40	60	100	35
7	22CY382	Vulnerability Assesment and Penetration Testing Lab	PC	0	2	1	40	60	100	36
8	22HS381/331	Advanced English Communication & Soft Skills Lab	HS	0	2	1	40	60	100	37
9	22CY383	Industrial Oriented Mini Project	PC	0	4	2	40	60	100	
			Total	**15**	**10**	**20**	**360**	**540**	**900**	
			Total Hours	**25**						

Note: Lecture Hours (L), Tutorials (T), Practicals (P), Drawing (D)

HS: HUMANITIES AND SOCIAL SCIENCES	**PE: PROFESSIONAL ELECTIVE**
ES: ENGINEERING SCIENCES	**BS: BASIC SCIENCES**
PC: PROFESSIONAL CORE	**MC: MANDATORY COURSE**

IV B.Tech. CSE (Cyber Security)

I Semester Course Structure

Regulations: R22(CBCS) **Admission to I B.Tech : 2022-23** **With effect from 2025-26 Onwards**

Sl. No.	Course Code	Courses	Category	Periods per Week		Credits	Scheme of Examination Maximum Marks			Pg. No.
				L	T/P/D		CIE (Continuous Internal Evaluation)	SEE (Semester End Examination)	Total	
1	22HS404/451	Organizational Behaviour	HS	3	0	3	40	60	100	39
2	22CY401	Ethical Hacking	PC	3	0	3	40	60	100	41
3	**Professional Elective - II:**									
	22DT402	Software Project Management	PE	3	0	3	40	60	100	43
	22CY402	Network Management Systems and Operations								45
	22CY403	Cyber Laws								47
	22CY404/356	Biometrics for Security								49
4	**Professional Elective - III:**									
	22IT403	Quantum Computing	PE	3	0	3	40	60	100	50
	22CY405	Blockchain Technologies								52
	22IT404	Cloud Security								54
	22CY406	Authentication Techniques								56
5	**Open Elective - I:**		OE	3	0	3	40	60	100	
Practicals										
6	22DT434/382	Big Data Analytics Lab	PC	0	2	1	40	60	100	58
7	22CY431	Ethical Hacking Lab	PC	0	2	1	40	60	100	59
8	22CY432	Project Stage-1	PC	0	6	3	40	60	100	
			Total	**15**	**10**	**20**	**320**	**480**	**800**	
			Total Hours	**25**						

Service courses of IV year I sem										
Sl. No.	Course Code	Courses	Branch	Category	Periods per Week		Credits	Scheme of Examination Maximum Marks		
					L	T/P/D		Internal	External	Total
1	22CY407	Fundamentals of Computer Networks	EIE	PE	3	0	3	40	60	100
2	22CY405	Blockchain Technologies	CSE, IT	PE	3	0	3	40	60	100
3	22CY404/356	Biometrics for Security	IT	PE	3	0	3	40	60	100

Note: Lecture Hours (L), Tutorials (T), Practicals (P), Drawing (D)

HS: HUMANITIES AND SOCIAL SCIENCES	**PE: PROFESSIONAL ELECTIVE**
ES: ENGINEERING SCIENCES	**BS: BASIC SCIENCES**
PC: PROFESSIONAL CORE	**MC: MANDATORY COURSE**

IV B.Tech. CSE (Cyber Security)

II Semester Course Structure

Regulations: R22(CBCS) Admission to I B.Tech : 2022-23 With effect from 2025-26 Onwards

Sl. No.	Course Code	Courses	Category	Periods per Week		Credits	Scheme of Examination Maximum Marks			Pg. No.
				L	T/P/D		CIE (Continuous Internal Evaluation)	SEE (Semester End Examination)	Total	
1	**Professional Elective - IV:**									
	22CY451	Data Analytics for Fraud Detection	PE	3	0	3	40	60	100	60
	22CY452	5G Technologies								61
	22CY453	Web Security								63
	22CY454	Database Security								64
2	**Professional Elective - V:**									
	22IT451	Design Patterns	PE	3	0	3	40	60	100	66
	22CY455	Cyber Forensics								67
	22CY456	Social Media Security								69
	22DT455	Information Storage Management								70
3	**Open Elective - II:**		OE	3	0	3	40	60	100	
4	22CY481	Project Stage-II	PC	0	22	11	40	60	100	
			Total	**9**	**22**	**20**	**160**	**240**	**400**	
			Total Hours	**31**						

Service courses of IV year II sem										
Sl. No.	**Course Code**	**Courses**	**Branch**	**Category**	**Periods per Week**		**Credits**	**Scheme of Examination Maximum Marks**		
					L	**T/P/D**		**Internal**	**External**	**Total**
1	22CY454	Database Security	**CSE(DS)**	**PE**	**3**	**0**	**3**	**40**	**60**	**100**
2	22CY455	Cyber Forensics	**CSE**	**PE**	**3**	**0**	**3**	**40**	**60**	**100**

Note: Lecture Hours (L), Tutorials (T), Practicals (P), Drawing (D)

HS: HUMANITIES AND SOCIAL SCIENCES
ES: ENGINEERING SCIENCES
PC: PROFESSIONAL CORE

PE: PROFESSIONAL ELECTIVE
BS: BASIC SCIENCES
MC: MANDATORY COURSE

22CY301

FOUNDATIONS OF CRYPTOGRAPHY

Instruction	:	3 Periods/Week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Evaluation	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** To Develop the competency in mathematical modeling, required for Cryptographic Algorithms
2 **:** To Build the Classical Encryption Techniques in the Cryptography
3 **:** To Explore basic security related aspects at the Network Endpoint

Unit-I

Information and Network Security Concepts: Cyber Security, Information Security and Network Security, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, Cryptography, Network Security, Trust and Trustworthiness, Standards.

Unit-II

Introduction to Number Theory: Divisibility and The Division Algorithm, The Euclidean Algorithm, Modular Arithmetic, Prime numbers, Fermat's and Euler's theorem, Testing for Primality, The Chinese Remainder Theorem, Discrete Logarithms.
Finite Fields: Groups, Rings and Fields, Finite Fields of the Form GF(p), Polynomial Arithmetic, Finite Fields of the Form(2^n).

Unit-III

Random Bit Generation and Stream Cipher
Principles of Pseudorandom Number Generation: The use of Random Numbers, TRNGs, PRNGs and PRFs, PRNG Requirements, Algorithm Design, Pseudorandom Number Generators: Linear Congruential and Blum Blum Shub generators, Stream Cipher, True Random Number Generators: Entropy Sources, Comparison of PRNGs and TRNGs, Conditioning, Health Testing, Intel Digital Random Number Generator.

Unit-IV

Classical Encryption Techniques
Symmetric Cipher Model, Substitution Techniques: Caesar, Mono-alphabetic, Playfair, Hill, Poly-alphabetic and One-Time Pad Cipher. Transposition Techniques: Rail Fence, Traditional Block Cipher Structure, Block Cipher Design Principles, Block Cipher Operations: Electronic Code Book, Cipher Block Chaining Mode, Counter Feedback Mode, Output Feedback Mode, Counter Mode.

Unit–V

Network Endpoint Security:
Firewalls: Characteristics, Types, DMZ Networks, Intrusion Detection System: Basic Principles, Approaches to Intrusion Detection, Host-Based Intrusion Detection Techniques, Network-Based Intrusion Detection Systems, Malicious Software: Types of Malware, Malware Defense, Distributed Denial of Service Attacks: DDoS Attack Description, Construction of the Attack Network, DDoS Countermeasures.

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Discuss Information & Network Security principles to familiarize with security aspects in the system

CO 2 : Apply Number Theory and Finite Fields concepts with respect to Asymmetric and Symmetric Ciphers.

CO 3 : Illustrate the Random Bit Generation and Stream Cipher in the context of Keyless and Single Key Cryptographic Algorithms

CO 4 : Model Classical Encryption Techniques and Block Cipher operations in Single Key Cryptography

CO 5 : Demonstrate the Network Endpoint Security in both Centralized and Decentralized Environment

Textbooks:

1. Cryptography and Network Security: Principles and Practice, W. Stallings, 8th Edition, Pearson, 2022.
2. Cryptography and Network Security, B. A. Forouzan and D.Mukhopadhyay, 2nd Edition, TMH, 2010.

References:

1. Cryptography & Network Security, Atul Kahate, 3rdEdition, TMH, 2013
2. Cryptography Theory and Practice, Stinson and Paterson,4th Edition, CRC Press, 2019.
3. Network Security: The Complete Reference, Robert Bragg, Mark Rhodes, TMH, 2008.

22CY302

MALWARE ANALYSIS AND DETECTION

Instruction	:	3 Periods/Week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Evaluation	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** Fundamentals of malware life cycle and Analysis setup
2 **:** Learn about the malware components and distribution mechanism
3 **:** Understand the static and dynamic analysis of malwares, malware detection.

Unit–I

Introduction: Types of Malware, Malware attack Life Cycle, Malware Business model, Malware Analysis setup, Operating Systems Files and File formats

Unit–II

System Fundamentals: Virtual memory and Portable Executable Files, Windows Internals – Win32 API, Registry, Directories, Processes and services.

Unit–III

Malware Components: Malware Components, Distribution mechanisms, Malware Packers, Persistence mechanism, Network Communication, Detecting Network Communication, Code Injection, Process Hollowing, API Hooking, Stealth techniques and Rootkits.

Unit–IV

Malware Analysis and Classification: Static Analysis, Dynamic Analysis, Memory Forensics with Volatility, Malware Payload dissection and Classification.

Unit–V

Malware Reverse Engineering: Debuggers and disassembly, Debugging for unpacking malware and code injections, Armoring Techniques Detection Engineering: Device Analysis, Anti-Virus Engines, IDS/IPS and Snort /Suricata rule writing, Malware Sandbox Internals, DBI for Malware analysis.

Course Outcomes: At the end of the course, the student should be able to

CO 1	:	Understand the malware and life cycle and Analysis setup
CO 2	:	Apply the distribution mechanism in malware analysis
CO 3	:	Discuss the static and dynamic analysis of malwares
CO 4	:	Analyze the malware detection methods and reverse engineering approaches
CO 5	:	Comprehend reverse engineering of malware and anti-malware analysis techniques

Textbooks:

1. Malware Analysis and Detection Engineering: A Comprehensive Appraoch to Detect and Analyze Modern Malware, Ahijit Mohanta, Anoop Saldanha, Apress Berkeley, CA, 2020

2. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, Michael Sikorski and Andrew Honig, No Starch Press, 2012.

References:

1. Learning Malware Analysis- Explore the concepts, tools, and techniques to analyze and investigate Windows malware, Monnappa K A, 1st edition, Packt Publishing, (ISBN 978-1-78839-250-1), United Kingdom, 2018.
2. Malware Analysis and Detection Engineering a Comprehensive Approach to Detect and Analyze Modern Malware, Abhijit Mohanta, Anoop Saldanha, 1st edition, Apress (ISBN 978-1-4842-6192-7), United States, 2020.

22IT301

WEB TECHNOLOGIES

(Common to IT, CSE, CSE-AI&ML, CSE-CS and CSE-DS)

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Prerequisites:

1. Must have knowledge in HTML 5 and CSS 3.
2. Must be knowledgeable on Java Technology.
3. Must be knowledgeable on any RDBMS.

Course Objectives:

1 **:** To learn a framework to create responsive web designing
2 **:** To learn the client-side script and validations along with a synchronous programming
3 **:** To introduce XML and work with data storage and interactivity using Java
4 **:** To introduce Server-side programming with Java Servlets
5 **:** To learn sending Dynamic Response from server using JSP

Unit-I–Working with CSS and its Framework

Introduction to CSS: Syntax structure, using style sheets, Box model. **CSS3:** Grid, Flexbox. Responsive Web Design using Media Queries, use of viewport, Transition, Animation.

CSS Framework: Bootstrap.

CSS Framework: Bootstrap (local and CDN usage, containers, 12 – column grid system, commonly used controls – Typography, Nav, Navbar, Carousel, Button, Card, Modal dialog, Table, forms, Breadcrumbs).

Unit-II– Client- Side Scripting Using JavaScript

JavaScript: Introduction to JavaScript, Data types, var, let, const., Control statements, Operator, Functions, fatarrows, Arrays, Objects, Destructuring, Strings, DateObjects, Events, DOM Manipulations, Regular Expressions.
Introduction to jQuery: Syntax, Selectors, Events, Effects.

Unit-III–Data storage and manipulation

XML: Syntax, namespaces, DTD, Schema, XML Document Parsing.
JDBC: Design of JDBC, JDBC Configuration, working with JDBC Statements, Scroll able and Updatable Result Sets, Rowset, MetaData, Transactions.

Unit-IV–Server-side Script ingusing Servlets

Webservers: An introduction to Web Servers, Web application structure and deployment in Tomcat. MVC Architecture, Servlet Technology: Servlets, Servlet sslife cycle, The Servlet API packages and class and interface hierarchy, Basic servlet program template, Handling requests and responses, using form parameters, Using Servlet Context and Servlet Config objects, Using initialization parameters (both context and configlevel), Session management(Cookies, HttpSession, URLRewriting, Hidden Formfields).

Unit-V–Dynamic Response using JSP

Introduction to JSP: The Anatomy of a JSP Page, JSP Processing, Declarations, Directives, Expressions, Code Snippets, implicit objects, Using Beans in JSP Pages, Using Cookies and session for session tracking, connecting to database in JSP.

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Build a custom website with HTML, CSS and Bootstrap
CO 2 : Demonstrate Java Script and it’s a synchronous nature of execution
CO 3 : Implement the Database Connectivity and Component Technologies like Beans. Develop and deploy Servlet based web applications
CO 4 : Develop Server-side programming using JSP
CO 5 : Build a custom website with HTML, CSS and Bootstrap

Textbooks:

1. Sams Teach Yourself HTML, CSS, and JavaScript AllinOne, Julie C.Meloni, JenniferKyrnin, 3rd Edition, Pearson Publication, 2019.
2. Head First Servlets and JSP, Bryan Basham, Kathy Sierra and BertBates, 2nd Edition, O’Reilly Media, 2008.
3. Core Java® Volume II—Advanced Features, CayS. Horstmann, 10th Edition; Printice Hall Publications, 2017

References:

1. Responsive Web Design with HTML5 and CSS3, BenFrain, 2nd Edition, Packt Publishing, 2015.
2. Beginning HTML, XHTML, CSS and JavaScript, JonDuckett, WileyPublishing, Inc.,2010.
3. Core Servlets and JSPs Volume I and II, Martin Hall and Larry Brown, Pearson.
4. E–Resource: https://www.w3schools.com/html/
5. E–Resource: https://developer.mozilla.org/en-US/docs/Learn/JavaScript
6. E–Resource: https://getbootstrap.com/

22CY303

IOT AND SECURITY SERVICES

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** To demonstrate the various python packages and IoT physical devices.
2 **:** To understand about SDN, IoT, M2M and various phases of the IoT security lifecycle
3 **:** To impart various IoT security threats and the measures to counter them.

Unit-I: Introduction to Internet of Things

Introduction - Definition and Characteristics of IoT, Physical Design of IoT, IoT Protocols. Logical Design of IoT, IoT Communication Models, IoT Communication APIs. IoT Levels and Deployment Templates. Sensors, Characteristics of Sensors, Classification of Sensors, challenges of IOT, Introduction to connectivity technologies, IEEE 802.15.4.47, ZIGBEE, 6LOWPAN, RFID, BLUETOOTH, Z-WAVE.

Unit-II: Python packages

JSON, XML, HTTPLib, URLLib, SMTPLib, RPi.GPIO.
IoT Physical Devices and Endpoints - Introduction to Raspberry PI, Interfaces (serial, SPI, I2C). Programming Raspberry PI with Python - Controlling LED, interfacing an LED and Switch, Interfacing a Light Sensor with Raspberry Pi.

Unit-III: SDN, IoT and M2M

SDN - Introduction, Limitations of current Network, origin of SDN, SDN architecture, Rule placement, Open Flow protocol, Controller Placement, Security in SDN, Integrating SDN in IOT.
IoT and M2M – Introduction – M2M, Difference between IoT and M2M, SDN and NFV for IoT.

Unit-IV: IoT Security

IoT Security- Vulnerabilities, Attacks and Countermeasures, Primer on Threats, Vulnerability and Risks (TVR), Primer on attacks and countermeasures, Today's IoT attacks, Lessons learned and systematic approaches.

Unit-V: Security Engineering for IoT Development and IoT Security Lifecycle

Security Engineering for IoT Development- Security Engineering for IoT Development, Building security in to design and development, Secure design, Processes and agreements, Technology selection – security products and services.
IoT Security Lifecycle - The IoT Security Lifecycle, The secure IoT system implementation lifecycle, Operations and maintenance, Dispose.

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Understand the characteristics, protocols and communication models required for logical design of IoT
CO 2 : Realize the hardware platforms for implementing and interfacing the IoT based board with different peripheral devices and serial communication devices.
CO 3 : Gain knowledge on protocol stacks for IoT, M2M and SDN
CO 4 : Familiarize various characteristics of IoT Security
CO 5 : Implement security life cycle for IoT devices

Textbooks:

1. Internet of Things - A Hands-on Approach, ArshdeepBahga and Vijay Madisetti, Universities Press,2015.
2. Practical Internet of Things Security, Brian Russell and Drew Van Duren, Packt Publishing, 2016.

References:

1. Internet of things, Jeeva Jose, 1st edition, Khanna publications, 2018.
2. Getting Started with Raspberry Pi, Matt Richardson & Shawn Wallace, O'Reilly (SPD), 2014.
3. IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices, Aaron Guzman and Aditya Gupta, Packt Publishing, 2017.
4. The IoT Hacker's Handbook a Practical Guide to Hacking the Internet of Things, Aditya Gupta, Apress, 2019.

.

22CS309/354

AUTOMATA THEORY AND COMPILER DESIGN

(Common to CSE, CSE-AI&ML, CSE-CS and CSE-DS)

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** To introduce the concepts of regular languages, finite automata, regular expressions, and context free grammar

2 **:** To make the students understand and implement top-down and bottom-up parsers

3 **:** To make the students understand the intermediate code forms, type checking

4 **:** To acquire knowledge on storage allocation strategies, symbol table management and code generation algorithms

5 **:** To introduce the concepts of regular languages, finite automata, regular expressions, and context free grammar

Unit-I: Introduction to Automata

Languages, definitions, Regular Expressions, Regular Grammars, Acceptance of Strings and Languages, Finite Automaton Model, DFA, NFA, conversion of NFA to DFA, Conversion of Regular Expression to NFA, Chomsky hierarchy of Languages.

Unit-II: Lexical Analysis and Top-down Parsing

Phases of compilation over view, Pass, Phase, Interpretation, Bootstrapping. Context free grammars, Top-down Parsing: Parse Trees, Ambiguous Grammars, Back tracking, LL (1), Recursive Descent parsing, Predictive parsing, pre-processing steps for predictive processing.

Unit-III: Bottom-Up Parsing and Syntax Directed Translation

Bottom-up parsing and handle pruning, LR(k)grammar parsing, LALR(k)grammars, Error Recovery in parsing, parsing ambiguous grammars, YACC parser generator.
Syntax Directed Translation, Attribute Grammars, Evaluation order for SDDs, Syntax Directed Translation schemas, Intermediate source program forms-AST, polish notation and 3 address code, DAG, Types and declarations, Type Checking, Equivalence of type expressions.

Unit-IV: Code Optimization

Symbol table format, organization, Block structured languages, hashing, Block structure and non-block structure storage allocation: static, runtime and heap allocation for arrays, strings, and activation records.
Consideration for optimization, Scope of optimization, DAG representation, Basic blocks, partitioning into basic blocks, Flowgraphs, Compile Time Evaluation, Common Sub expression elimination, dead code elimination, Strength Reduction, Code Movement, Loop Invariant Method, Loop Fusion, Loop Unrolling, Induction Variables and Reduction in Strength.

Unit-V: Code Generation

Absolute Code, Assembler Code, Register and Address Descriptors, Implementing Global Register Allocation, Usage Counts, Using DAG for register allocation, Simple Code Generation Algorithm, Generic Code generation Algorithm.

Course Outcomes: At the end of the course, the student should be able to

CO 1: Covert NFA to DFA and regular expression to DFA

CO 2: Design top-down and bottom-up parsers

CO 3: Understand the concepts of type checking and intermediate code generation forms

CO 4: Understand the concepts of storage allocation strategies, symbol table management and hashing

CO 5: Use DAG for generating assembly language code and able to generate relocatable machine code

Textbooks:

1. Introduction to Automata Theory Languages and Computation, Hopcroft H.E. and Ullman J.D., Pearson Education, 2009.
2. Principles of Compiler Design, A. VAho and JD Ullman, Pearson Education, 2002.

References:

1. Compiler Construction: Principles and Practice, Kenneth C.Louden, Thomson/Delmar Cengage Learning, 2006.
2. Lex & yacc, Doug Brown, John Levine and Tony Mason, 2nd Edition, O'reilly Media, 1992.
3. Engineering a compiler, Keith Cooper and Linda Torczon, 2nd Edition, MorganKaufmann, 2011.
4. Modern Compiler Construction in C, Andrew W. Appel, Cambridge University Press, 2004

22IT331

WEB TECHNOLOGIES LAB

(Common to IT, CSE, CSE-AI&ML, CSE-CS and CSE-DS)

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	1.5	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** To learn the basics of HTML elements, java Console and GUI based programming

2 **:** To introduce XML and processing of XML Data with Java

3 **:** To introduce Server-side programming with Java Servlets and JSP, Client-side scripting with JavaScript and AJAX.

Exercises:

1. Create a web page using the advanced features of CSS: Grid, Flexbox. And apply transition and animations on the contents of the web page.
2. Make the web pages created in the above experiment as responsive web page with Bootstrap Framework.
3. Validate the registration, user login, user profile and payment pages using JavaScript. Make use of any needed JavaScript objects.
4. Build a scientific calculator.
5. JavaScript Program to demonstrate working of prototypal inheritance, closure, callbacks, promises and async / await.
6. Write an XML file which will display the Book information with the following fields: Title of the book, Author Name, ISBN number, Publisher name, Edition, Price
7. Define a Document Type Definition (DTD) and XML schema to validate the above created XML Documents
8. Write a java program to establish a connection to a database and execute simple SQL queries.
9. Write a java program to demonstrate the usage of JDBC in performing various DML statements. Use prepared statements and callable statements.
10. Write a java-based application to demonstrate the Updatable and Scrollable result sets.
11. Write a java program to access meta data of the SQL database.
12. Write a program to accept request parameters from a form and generate the response.
13. Write a program to accept Servlet Config and Servlet Context parameters.
14. Assume four users user1, user2, user3 and user4 having the passwords pwd1, pwd2, pwd3 and, pwd4 respectively. Write a servlet for doing the following functionalities.
    a. Create a Cookie and add these four user ids and passwords to this Cookie.
    b. Read the user id and password entered into the Login form and authenticate with the values (user id and passwords) available in the cookies. If the person is a valid user (i.e., user-name and password match) you should welcome by name (user-name) else you should display the message "You are not an authenticated user ".
15. Develop a servlet to demonstrate the database access and update from a database.
16. Create a servlet to implement an authentication filter mechanism.
17. Develop a servlet to implement servlet context and session listeners.
18. Write a JSP which does the following job:
    a. Insert the details of the three users who register with the web site by using registration form.
    b. Authenticate the user when he submits the login form using the username and password from the database.
19. Write a JSP to demonstrate the usage of JSP standard actions.
20. Write a JSP to show the usage of various scripting elements.
21. Design and use a custom tag library.
22. Design a simple application using both Servlets and JSPs along with database access.

Note: Programs from 1 to 14 are mandatory and Programs from 15 to 22 are optional.

Course Outcomes: At the end of the course, the student should be able to

CO 1 : To build a custom website with HTML, CSS, and Bootstrap
CO 2 : Demonstrate JavaScript, XML, DHTML and related Technologies
CO 3 : Implement the Database Connectivity and Component Technologies like Beans
CO 4 : Deploy the servlet technology & API Management
CO 5 : Construct the fundamentals of JSP

References:

1. Beginning HTML, XHTML, CSS, and JavaScript, Wrox Publications, 2010
2. Head First Servlets and JSP, Bryan Basham, Kathy Sierra and Bert Bates, 2nd Edition, O'Reilly Media, 2008.
3. Core Java: Volume II – Advanced Features, Cay Horstmann and Gary Cornell, 9th Edition, Prentice Hall, 2013 (Only Chapter 4 for Database Programming)

22CY331

CRYPTOGRAPHY AND COMPILER DESIGN LAB

Instruction	:	3 Periods/Week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Evaluation	:	60 Marks
Credits	:	1.5	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** To Implement the Asymmetric Cryptography related Mathematical Concepts
2 **:** To Realize the Classical Encryption Techniques through programming practice
3 **:** To enable the students to simulate a simple compiler for arithmetic expressions

List of Experiments

1. Write a Java Program to implement the Chinese Remainder Theorem.
2. Write a Java Program to implement Discrete Logarithmic Problem.
3. Write a Java Program to generate Pseudorandom Number using Linear Congruential Method.
4. Write a Java Program to demonstrate Caesar Cipher technique.
5. Write a Java Program to implement Play Fair Cipher technique.
6. Write a Java Program to implement Hill Cipher technique.
7. Write a Java Program to implement Rail Fence technique.
8. Develop a lexical analyzer to recognize a few patterns in c (ex. Identifiers, constants, comments, operators, etc.…….).
9. Implementation of Calculator using LEX and YACC.
10. Write a C program to generate three address code.
11. Write a C program to implement a top-down parser (Recursive Descent Parser).
12. Write a C program to implement OPERATOR PRECEDENCE PARSING.
13. Write a C program to generate a three address code for a given expression.
14. Write a C program to generate an assembly language instruction from three address code.
15. Implementation of simple code optimization techniques (constant folding. etc.)

Course Outcomes: At the end of the course, the student should be able to

CO 1	:	Interpret Mathematical concepts related to Asymmetric Cryptographic Techniques
CO 2	:	Demonstrate Random Bit Generation technique using Keyless Cryptographic
CO 3	:	Illustrate Substitution and Transposition Techniques of the Classical Single Key Cryptography
CO 4	:	Implement a hand coded lexical analyser and enhance it using LEX tool
CO 5	:	Implement an efficient parse Tree co-construction program using YACC tool

Textbooks:

1. Cryptography and Network Security: Principles and Practice, W. Stallings, 8th Edition, Pearson, 2022.
2. Cryptography and Network Security, B. A. Forouzan and D.Mukhopadhyay, 2nd Edition, TMH, 2010.
3. Compilers: Principles, Techniques and Tools, Alfred V. Aho, Monica S. Lam, Ravi Sethi, Jeffry D. Ullman, 2nd Edition.

22CY332

IOT AND SECURITY SERVICES LAB

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	1.5	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** To develop an understanding of the basic concepts of IOTs
2 **:** To explore different Raspberry Pi operating systems, and Raspberry PI hardwar
3 **:** To realize and implement IOT functionalities

List of Experiments:

1. Start Raspberry Pi and try various Linux commands in command terminal window:
   a) ls, cd, touch, mv, rm, man, mkdir, rmdir, tar, gzip, cat, more, less, ps, sudo, cron
   b) chown, chgrp, ping etc.
2. Perform necessary software installation on Raspberry Pi.
3. Interface LED/Buzzer with Raspberry Pi, write a program to turn ON LED for 1 sec after every 2 seconds.
4. Interface Push button/Digital sensor (IR/LDR) with Raspberry Pi, write a program to turn ON LED when push button is pressed or at sensor detection.
5. Interface DHT11 sensor with Raspberry Pi, write a program to print temperature and humidity readings.
6. Interface DHT11 sensor with Raspberry Pi, write a program to print temperature and humidity readings.
7. Interface motor using relay with Raspberry Pi, write a program to turn ON motor when push button is pressed.
8. Interface soil moisturizer sensor using relay with Raspberry Pi, write a program to find the amount of moist in soil.
9. Write a program on Raspberry Pi to upload temperature and humidity data to cloud.
10. Capture and Analyse system network traffic.
11. Perform foot printing, information gathering using various foot printing tools.

Course Outcomes: At the end of the course, the student should be able to

CO 1	:	Setting up Raspberry Pi and connect to a network
CO 2	:	Familiarization with GPIO pins and Control hardware through GPIO pins
CO 3	:	Use sensos to measure temperature, humidity, light and distance
CO 4	:	Deploy an IOT application and connect to the cloud
CO 5	:	Design IOT based prototypes with Raspberry pi using python

Textbooks:

1. Internet of Things - A Hands-on Approach, Arshdeep Bahga and Vijay Madisetti, Universities Press, 2015.
2. Internet of things, Jeeva Jose, 1st Edition, Khanna publications, 2018.
3. Getting Started with Raspberry Pi, Matt Richardson & Shawn Wallace, O'Reilly (SPD), 2014.

22CY333

ADVANCED WEB PROGRAMMING LAB

(Common to CSE-AI&ML, CSE-CS and CSE-DS)

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	1.5	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** Able to develop web applications and learn the principles of server-side scripting with Node.js

2 **:** Understanding Components and Event handling in React, create react applications and React forms

3 **:** Working with applications consuming REST APIs

Exercises:

1. Create a git repository and clone it for changes and publish the changes using git bash.
2. Create a realtime database in firebase for the student management system and explore the features of Firebase Real Time Database.
3. Explore the various node modules: os, http, etc.
4. Create a REST API and perform various CRUD operations on that.
5. Develop an express web application that can interact with a service to perform CRUD operations on student data. (Use Postman)
6. For the above application create authorized end points using JWT (JSON Web Token).
7. Create a react application using create-react-app and display "Hello World". (ReactJS environment Setup using Node Package Manager, Motivation for using React, Virtual DOMvs Real DOM).
8. Create a react application to render the element with the current system date and time. (Introduction to JSX and its uses,Expressions in JSX,Rendering Elements in React.JS. ReactDOM. render() function. How does render function work and update DOM)
9. a. Create a functional component that accept the arbitrary inputs (called props) and display the value.

   b. Create a class component that accept the arbitrary inputs (called props) and display the value.

   (Introduction to Components in React, Types of Components in react, Functional vs Class Component, Passing the props to child Components).
10. Create a class component that accept the date in the form of State and displays the date.

    (Passing the state to Class Component, Props vs State).
11. Create a react application to demonstrate the component lifecycle.

    (Understanding the Lifecycle Methods: Phases of React Component Lifecycle, React Component Lifecycle methods)
12. Create a react application to create a two buttons and handle the click events. The click event of first display the current system date and time using event listener (Normal functions). For click event of second button display "Good Bye" by using event listener (arrow functions)

    (Handling the events in React, Binding event listeners)
13. Create a react application to implement the calculator application by creating UI and providing the functionality using events. Also make it look good by using styles.

    (React Styling: How to use the Styles in React)
14. Create a react application to create a registration page using forms as controlled components.

    (Working with the React Forms)
15. Create a react application to understand how the React Router works. The application will contain four components: home component, product component, about component, and contact component. We will use React Router to navigate between these components.

    (React Rounting, React Router components)

16. Create a simple e-commerce storefront for a bookstore which consists of four screens:
    Home —The storefront with a book list
    Product page —A separate product page
    Cart —A web page showing the quantities and titles selected by the user
    Checkout—A print-ready invoice with the list of books
17. Access a web service in react that fetches the weather information from open weather map and the display the current and historical weather information using graphical representation using chart.js.
    (Consuming the REST APIs in the React)
18. Create a TODO application in react with necessary components and deploy it into github.

Course Outcomes: At the end of the course, the student should be able to

CO 1	:	To design and build robust REST APIs using Node.js, demonstrate the Express Framework
CO 2	:	Understand components in React
CO 3	:	Handle event in React and bind event listeners
CO 4	:	Work with React forms
CO 5	:	Create applications for consuming REST APIs

References:

1. *React Quickly*, Azat Mardan, Manning Publications, August 2017.
2. *Pro MERN Stack, Full Stack Web App Development with Mongo, Express, React, and Node,* Vasan Subramanian, 2nd Edition, APress, 2019.

22HS302/352/253

INTELLECTUAL PROPERTY RIGHTS

(Common to CE, EIE, ECE, IT, ME, EEE and CSE-AI&ML, CSE-CS, CSE-DS)

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	100 Marks
Tutorial	:	-	Semester End Examination	:	-
Credits	:	0	Semester End Exam Duration	:	-

Course Objectives:

1 : To impart basic concepts in IPR
2 : To understand the various aspects of Trade Marks
3 : To create awareness on Law of Patents and Copyrights
4 : To highlight relevance of Trade Secrets in any Trade/Business
5 : To get elementary knowledge of International IPRs and New developments in IPR

Unit- I - Introduction to Intellectual property

Introduction, types of intellectual property, international organizations, agencies and treaties, importance of intellectual property rights.

Unit -II - Trade Marks

Purpose and function of trademarks, acquisition of trademark rights, protectable matter, selecting, and evaluating trademark, trade mark registration processes.

Unit -III - Law of copyrights

Fundamental of copy right law, originality of material, rights of reproduction, rights to perform the work publicly, copy right ownership issues, copy right registration, notice of copy right, international copy right law.
Law of patents: Foundation of patent law, patent searching process, ownership rights and transfer

Unit -IV- Trade Secrets

Trade secrete law, determination of trade secrete status, liability for misappropriations of trade secrets, protection for submission, trade secrete litigation.
Unfair competition: Misappropriation right of publicity, false advertising.

Unit -V- New development in intellectual property

New developments in trademark law; copy right law, patent law, intellectual property audits. International overview on intellectual property, international – trademark law, copy right law, international patent law, and international development in trade secrets law.

Course Outcomes: At the end of the course, the student should be able to

CO 1	:	Understand concepts of intellectual property rights
CO 2	:	Evaluate trademark
CO 3	:	File for a patent
CO 4	:	Analyze the fairness in a competition
CO 5	:	Understand laws related to intellectual property rights

Textbooks:

1. Intellectual Property right, Deborah. E. Bouchoux, 4th Edition, Cengage learning, 2012.
2. Intellectual Property right – Unleashing the knowledge economy, Prabuddha Ganguli, 1st Edition, Tata McGraw Hill Publishing company ltd, 2017.

References:

1. Intellectual Property Patents, Trademarks and Copyrights, Richard Stim, 2nd Edition, Cengage learning, 2012.
2. Intellectual Property Rights under WTO, T. Ramappa, S. Chand, 2008.

22CY351

CRYPTOGRAPHY AND NETWORK SECURITY

Instruction	:	3 Periods/Week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Evaluation	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** To Illustrate the Functionality of Symmetric, Asymmetric Ciphers, Hashing, MAC and Digital Signatures

2 **:** To Demonstrate the Security Protocols in the Network, Transport and Application Layers.

3 **:** To Relate the realization of User Authentication Protocols and Key Management & Distribution using Symmetric and Asymmetric Cryptography

Unit-I

Symmetric Ciphers: The Data Encryption Standard (DES), The Strength of DES, The Advanced Encryption Standard (AES): AES Structure, AES Transformation Functions, AES Key Expansion,
RC4: Initialization of S, Stream Generation, Strength of RC4.
Asymmetric Ciphers: Principles of Public-Key Cryptosystem, The RSA Algorithm, Diffie-Hellman Key Exchange, ElGamal Cryptographic System, Elliptic Curve Arithmetic, Elliptic Curve Cryptography.

Unit-II

Cryptographic Hash Functions: Applications of Cryptographic Hash Functions, Two Simple Hash Functions, Hash Functions Based on Cipher Block Chaining, SHA-512 Algorithm.
Message Authentication Codes: Message Authentication Requirements, Message Authentication Functions, Requirements for Message Authentication Codes, Security of MAC, HMAC, Digital Signatures, NIST Digital Signature Algorithm(DSA).

Unit-III

IP Security: IP Security Overview, IP Security Policy, Encapsulation Security Payload, Combining Security Associations, Internet Key Exchange.
Transport-Layer Security: Web Security Considerations. Transport Layer Security: Architecture, Record Protocol, Change Cipher Spec Protocol, Alert Protocol, Handshake Protocol, Cryptographic Computations, SSL/TLS Attacks, TLSv1.3

Unit-IV

Electronic Mail Security: Internet Mail Architecture, Email Formats, Email Threats, Comprehensive Email Security, S/MIME.

Cryptographic Key Management and Distribution

Symmetric Key Distribution Using Symmetric Encryption, Symmetric Key Distribution Using Asymmetric Encryption, Distribution of Public Keys, X.509 Certificates, Public Key Infrastructure.

Unit–V

User Authentication Protocols

Remote User Authentication Principles: The NIST Model for Electronic User Authentication, Means of Authentication, Multifactor Authentication, Mutual Authentication, Remote User Authentication Using Symmetric Encryption, Mutual Authentication. Kerberos: Motivation, Version 4, Version 5, Remote User Authentication Using Asymmetric Encryption, Mutual and One-Way Authentication

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Demonstrate the Operational Functioning of Symmetric and Asymmetric Cipher

CO 2 : Illustrate the working of Hashing Functions, MAC and Digital Signatures to ensure Data Integrity and Authentication

CO 3 : Discuss the Security Protocols adopted at the Network (IP) and Transport Layer

CO 4 : Illustrate the Application Layer Security Protocol and Key Management & Distribution Techniques

CO 5 : Apply Security Protocols to assure Remote User Authentication using Symmetric and Asymmetric Cipher

Textbooks:

1. Cryptography and Network Security: Principles and Practice, W. Stallings, 8th Edition, Pearson, 2022.
2. Cryptography and Network Security, B. A. Forouzan and D.Mukhopadhyay, 2nd Edition, TMH, 2010.

References:

1. Cryptography & Network Security, Atul Kahate, 3rd Edition, TMH, 2013.
2. Cryptography Theory and Practice, Stinson and Paterson, 4th Edition, CRC Press,2019.
3. Network Security: The Complete Reference, Robert Bragg, Mark Rhodes, TMH, 2008.

22CY352

VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** The tools that can be used to perform information gathering
2 **:** The various attacks in various domains of cyberspace
3 **:** The vulnerabilities associated with various network applications and database system

Unit-I: Information Gathering and Detecting Vulnerabilities

Open source intelligence gathering, port scanning, nessus policies, web application scanning manual analysis traffic capturing.
Introduction Ethics of Ethical Hacking: Why you need to understand your enemy's tactics, recognizing the gray areas in security, Vulnerability Assessment and Penetration Testing.

Unit-II: Attacks and Exploits

Password Attacks Client Side Exploitation Social Engineering, by passing Antivirus Applications. Metasploit Payloads Open php My Admin-Buffer overflow: Windows and Linux, Web scanning exploits, port Scanning exploits, SQL exploits.

Unit-III: Wireless Security

Wired vs wireless Privacy Protocols, Wireless Frame Generation Encryption Cracking Tools, Wireless DoS Attacks

Unit-IV: Common Vulnerability Analysis of Application Protocols

Simple Mail Transfer Protocol, File Transfer Protocol, Trivial File Transfer Protocol, Hyper Text Transmission Protocol, ICMP, SMURF, UDP, DNS, PING, SYN.

Unit-V: Penetration Tools and Database Security

Trace routes, Neo trace, what web. Database Security: Access control in database systems, Inference control multilevel database security.

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Make use of different OSINT Tools, Techniques and Resources that return better results for different kind of queries

CO 2 : Demonstrate wide variety of methodologies and standards of penetration testing that the vulnerabilities were discovered

CO 3 : Illustrate the attacking networks that deploy various security protocols in Wireless Security

CO 4 : Choose different techniques, protocols that can be used to perform the vulnerability analysis of web-based applications

CO 5 : List the different types of factors, control measures, mechanisms that defend against database security issues

Textbooks

1. Penetration Testing: A Hands on Introduction to Hacking, Georgia Weidman, 1st Edition, No Startch Press, 2014.
2. Gray Hat Hacking - The Ethical Hackers Handbook, Allen Harper, Stephen Sims, Michael Baucom, 3rd Edition, Tata Mc Graw-Hill.

3. Vulnerability Analysis and Defense for the Internet, B.Singh, H. Joseph and Abhishek Singh, Springer, 2008.

References:

1. Ethical Hacking and Penetration Testing Guide, Rafay Baloch, CRC Press, 2015,
2. The Basics of Hacking and Penetration Testing, Dr. Patrick Engebretson, Syngress Publications Elseveir, 2013.
3. Mastering Modern Web Penetration Testing, Prakhar Prasad, Packtet Publishing, 2016.
4. The Web Application Hacker's Handbook-Discovering and Exploiting Security flaws, Dafydd Suttard, Marcus pinto, 1st Edition, Wiley Publishing.

22CY353

CYBER CRIME INVESTIGATIONS AND DIGITAL FORENSICS

Instruction	:	3 Periods/Week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Evaluation	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** Understand the network protocols for communicating on IT networks and potential attacks at each layer of the TCP/IP Model

2 **:** understand the process of investigating cyber incidents

3 **:** To assist the students to identify malicious activities through log analysis and to trace the source of an IP Address using forensics techniques

Unit-I

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

Unit-II

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

Unit-III

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

Unit-IV

Digital Forensics: Introduction to Digital Forensics, Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition, Audio Video Analysis, Windows System Forensics, Linux System Forensics, Network Forensics.

Unit-V

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

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Understand the fundamentals of cybercrime

CO 2 : Explain various cybercrime issues and Digital Laws

CO 3 : Understand different Investigation Tools for Cybercrime

CO 4 : Understand basics of Forensic Technology and Practices

CO 5 : Analyze different laws, ethics and evidence handling procedures

Textbooks:

1. Computer Forensics and Investigations, Nelson Phillips and Enfinger Steuart, Cengage Learning, New Delhi, 2009.
2. Incident Response and Computer Forensics , Kevin Mandia, Chris Prosise, Matt Pepe, Tata McGraw -Hill, New Delhi, 2006.

References:

1. Software Forensics, Robert M Slade, Tata McGraw - Hill, New Delhi, 2005.
2. Cybercrime, Bernadette H Schell, Clemens Martin, ABC – CLIO Inc, California, 2004.
3. Understanding Forensics in IT , NIIT Ltd, 2005.

22HS351/301/401

BUSINESS ECONOMICS AND FINANCIAL ANALYSIS

(Common to ALL)

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** To obtain the knowledge about types of Business Structures and features
2 **:** To learn various principles of Managerial Economics and to make them effective business decision makers
3 **:** To make the students understand functional areas and potential problems in economics for efficient utilization of resources
4 **:** To have an overview on market structures and Competition
5 **:** To gain knowledge on important elements

Unit-I – Introduction to Business and Economics

Business: Structure of Business Firm, Theory of Firm, Types of Business Entities, Limited Liability Companies, Sources of Capital for a Company, Non-Conventional Sources of Finance. Economics: Significance of Economics, Micro and Macro Economic Concepts, Concepts and Importance of National Income, Inflation, Money Supply and Inflation, Business Cycle, Features and Phases of Business Cycle. Nature and Scope of Business Economics, Role of Business Economist, Multidisciplinary nature of Business Economics.

Unit-II - Demand and Supply Analysis

Elasticity of Demand: Elasticity, Types of Elasticity, Law of Demand, Measurement and Significance of Elasticity of Demand, Factors affecting Elasticity of Demand, Elasticity of Demand in decision making. Demand Forecasting: Characteristics of Good Demand Forecasting, Steps in Demand Forecasting, Methods of Demand Forecasting.
Supply Analysis: Determinants of Supply, Supply Function and Law of Supply.

Unit-III -Production, Cost, Market Structures & Pricing

Production Analysis: Factors of Production, Production Function, Production Function with one variable input, two variable inputs, Returns to Scale.
Cost analysis: Types of Costs, Short run and Long run Cost Functions.
Market Structures: Nature of Competition, Features of Perfect competition, Monopoly, Oligopoly, Monopolistic Competition.
Pricing: Types of Pricing, Product Life Cycle based Pricing, Break Even Analysis (Simple Problems)

Unit-IV –Financial Accounting

Accounting concepts and Conventions, Accounting Equation, Double-Entry system of Accounting, Rules for maintaining Books of Accounts, Journal, Posting to Ledger, Preparation of Trial Balance, Elements of Financial Statements, Preparation of Final Accounts (Simple Problems).

Unit-V – Financial Ratios Analysis

Concept of Ratio Analysis, Importance and Types of Ratios, Liquidity Ratios, Turnover Ratios, Profitability Ratios, Proprietary Ratios, Solvency, Leverage Ratios –Analysis and Interpretation (simple problems).

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Understand the concepts of micro and macro economics
CO 2 : Analyze demand and forecast demand
CO 3 : Evaluate markets and formulate competitive strategies
CO 4 : Prepare financial statements
CO 5 : Evaluate the financial strengths and weaknesses of a business by using ratio analysis

Textbooks:

1. Business Economics - Theory and Applications, D. D. Chaturvedi, S. L. Gupta, International Book House Pvt. Ltd. 2013.
2. Financial Accounting, Dhanesh K Khatri, Tata Mc –Graw Hill, 2011.
3. Managerial Economics, Geethika Ghosh, Piyali Gosh, Purba Roy Choudhury, 2nd Edition, Tata McGraw Hill Education Pvt. Ltd. 2012.

References:

1. Financial Accounting for Management, Paresh Shah, 2nd Edition, Oxford Press, 2015.
2. Financial Accounting, S. N. Maheshwari, Sunil K Maheshwari, Sharad K Maheshwari, 5th Edition, Vikas Publications, 2013.

22DT354

DATA WAREHOUSING AND BUSINESS INTELLIGENCE

(Professional Elective – I)
(Common to CSE-AI&ML, CSE-CS AND CSE-DS)

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** This course is concerned with extracting data from the information systems that deal with the day-to-day operations and transforming it into data that can be used by businesses to drive high-level decision making

2 **:** Students will learn how to design and create a data warehouse, and how to utilize the process of extracting, transforming, and loading (ETL) data into data warehouses.

3 **:** Equip students with skills of manipulating data warehouses to generate information for business decision making

Unit–I

DATA WAREHOUSE: Data Warehouse-Data Warehouse Architecture- Multidimensional Data Model Data cube and OLAP Technology-Data Warehouse Implementation -DBMS schemas for Decision support - Efficient methods for Data cube computation.

Unit–II

Business Intelligence: Introduction – Definition, Leveraging Data and Knowledge for BI, BI Components, BI Dimensions, Information Hierarchy, Business Intelligence and Business Analytics. BI Life Cycle. Data for BI - Data Issues and Data Quality for BI.

Unit-III

BI Implementation - Key Drivers, Key Performance Indicators and Performance Metrics, BI Architecture/Framework, Best Practices, Business Decision Making, Styles of BI-vent-Driven alerts – Acyclic process of Intelligence Creation. The value of Business Intelligence-Value driven & Information use.

Unit-IV

Advanced BI – Big Data and BI, Social Networks, Mobile BI, emerging trends, Description of different BI-Tools (Pentaho, KNIME)

Unit-V

Business intelligence implementation-Business Intelligence and integration implementation-connecting in BI systems- Issues of legality- Privacy and ethics- Social networking and BI.

Course Outcomes: At the end of the course, the student should be able to

CO 1	:	Explore the architecture of data warehouse and OLAP operations.
CO 2	:	Learn fundamental concepts of BI and Analytics
CO 3	:	Application of BI Key Performance indicators
CO 4	:	Utilization of Advanced BI Tools and their Implementation.
CO 5	:	Implementation of BI Techniques and BI Ethics.

Textbooks:

1. Data Mining – Concepts and Techniques - JIAWEI HAN & MICHELINE KAMBER, Elsevier.
2. Business Intelligence Rajiv Sabherwal, Wiley Publications, 2012.

References:

1. Decision Support and Business Intelligence Systems, Efraim Turban, Ramesh Sharda, Jay Aronson, David King, 9th Edition, Pearson Education, 2009.
2. Business Intelligence - The Savy Manager's Guide Getting Onboard with Emerging IT, David Loshin, Morgan Kaufmann Publishers, 2009.
3. Building Integrated Business Intelligence Solutions with SQL Server, 2008 R2 & Office 2010, Philo Janus, Stacia Misner, TMH, 2011.
4. Business Intelligence Data Mining and Optimization for decision making [Author: Carlo-Verellis] [Publication: (Wiley)].
5. Data Warehousing, Data Mining & OLAP- Alex Berson and Stephen J. Smith- Tata McGrawHill Edition, Tenth reprint 2007.
6. Building the Data Warehouse- W. H. Inmon, Wiley Dreamtech India Pvt. Ltd.
7. Data Mining Introductory and Advanced topics –MARGARET H DUNHAM, PEA.

22CY354

WIRELESS NETWORKS AND MOBILE COMPUTING

(Professional Elective-I)

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** To provide an introduction to mobile and wireless computing
2 **:** To provide a basic understanding of how the communication networks are planned, Managed, administered and operated
3 **:** To understand Communication management networks, protocols, modelling, network management applications such as configuration, fault and performance management

Unit-I - Introduction to Network Technologies and Cellular Communications: Infrared vs. Radio Transmission, Infrastructure and Ad Hoc Networks, GSM - Mobile services, System architecture, Radio interface, Protocols, Localization and calling, Handover, Security, and New data services.
Mobile Computing (MC) - Introduction to MC, novel applications, limitations, and architecture, Bluetooth - User Scenarios, Physical Layer, MAC layer, Networking, Security, Link Manager Protocols.

Unit-II - Medium Access Control: Motivation for a specialized MAC (Hidden and exposed terminals, near and far terminals), SDMA, FDMA, TDMA, CDMA, MAC protocols for GSM, Wireless LAN (IEEE802.11), collision Avoidance (MACA, MACAW) protocols.

Unit-III - Mobile IP Network Layer: IP and Mobile IP Network layers, IP Packet Delivery and Handover Management, Location Management Registration, tunnelling and encapsulation, Reverse tunnelling, Dynamic Host Configuration Protocol(DHCP).

Unit-IV - Mobile Transport Layer: Conventional TCP/IP Protocols, Indirect TCP, Snooping TCP, Mobile TCP, Other transport Protocols for Mobile Networks.

Unit-V – Mobile Ad hoc Networks (MANETs): Introduction, applications and challenges of a MANET, applications. Routing Protocols- Routing, Dynamic source routing, Destination sequence distance vector, Overview ad-hoc routing protocols, Application- RFID, Bluetooth, Zigbee, NFC.

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Apply advanced data communication methods and networking protocols for wireless and mobile environment
CO 2 : Utilize and employ application frame works for developing mobile applications including under disconnected and weakly connected environment
CO 3 : Select components and networks for particular application
CO 4 : Understand issues related to client server computing with adaptation, power aware and context aware computing and MANET Protocols
CO 5 : Have a good understanding of how the underlying wireless and mobile communication networks work, their technical features, and what kinds of applications they can support

Textbooks:

1. Mobile Communications, Jochen Schiller, 2nd Edition, Addison-Wisley, 2004
2. Mobile Computing Principles: Designing and Developing Mobile Applications with UML and XML, Reza Behravanfar, Cambridge University Press, October 2004.

References:

1. Mobile Computing, RajKamal, Oxford University Press, 2007.
2. Wireless Communication and Networking, William Stallings, PHI, 2003.

22AM357

FUNDAMENTALS OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE

(Professional Elective-I)

Instruction	:	3 Periods / week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:		Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** To develop an understanding of the basic concepts of Artificial Intelligence.
2 **:** To analyze the nature of various advanced search strategies in AI.
3 **:** To impart knowledge representation and Data preprocessing.

Unit-I - Introduction

Introduction to AI, Intelligent Agents.
Solving Problems by Search: Uninformed Search Strategies: Breadth-first search, Uniform cost search, Depth-first search.
Informed (Heuristic) Search Strategies: Greedy best-first search, A* search, Heuristic Functions, Search in complex environments: Local search and Optimization problems, Local Search in Continuous Spaces, Searching with Non-Deterministic Actions.
Adversarial Search: Optimal decisions in games, Heuristic Alpha-Beta search, Monte Carlo tree search.

Unit-II - Knowledge, Reasoning and Planning

Logic Agents: Based Agents, The Wumpus World, Logic, Propositional Logic, Propositional Theorem Proving.
First-Order Logic: Syntax and Semantics of First-Order Logic, Using First-Order Logic, Knowledge Engineering in First-Order Logic.
Inference in First-Order Logic: Propositional vs. First-Order Inference, Unification and Lifting, Forward Chaining, Backward Chaining, Resolution.

Unit-III - Knowledge Representation

Knowledge Representation: Ontological Engineering, Categories and Objects, Events. Mental Events and Mental Objects, Reasoning Systems for Categories, Reasoning with Default Information.
Introduction to Data Science: Data science, Characteristics of Bigdata, Different steps in Data science process, Data types, Similarity and dissimilarity measures, Data quality, Data Cleaning, Data Integration, Data Transformation.

Unit-IV - Multivariate Analysis:

Multivariate Methods: Mean Vector, Covariance, Correlation and Precision Matrices, Multivariate Data, Parameter Estimation, Estimation of Missing Values, Multivariate Normal Distribution.
Hypothesis testing: t-Test, z-Test, Chi-Square-Test.
Analysis of Variance (ANOVA): One-way, Two-way.
Stochastic Process: Poisson process, Compound Poisson process and Markov chains.

Unit-V - Data Science Applications

Applications in various domains, Challenges and opportunities, tools for data scientists.
Recommender systems: Introduction, methods, application, challenges.
Time series data: Stock market index movement forecasting. Supply Chain Management – Real world case study in logistics.

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Identify the scope for agent-based engineering solutions using AI based tools

CO 2 : Demonstrate advanced search strategies, perform search space reduction techniques using minmax algorithm

CO 3 : Apply knowledge representation, reasoning to AI-based solutions

CO 4 : Understand and apply multivariate data analysis techniques

CO 5 : To correlate data science and solutions to modern problems

Textbooks:

1. Artificial Intelligence A Modern Approach, Stuart Russel and Peter Norvig, 4th Edition, Pearson, 2020.
2. Data Science and its applications, Aakanksha Sharaff, G.K.Sinha, CRC Press, 2021.

References:

1. Data Mining: Concepts and Techniques, Jiawei Han and Micheline Kamber, 4th Edition, Morgan Kaufmann Publishers, 2023.
2. Business Analytics, U. Dinesh Kumar, Wiley publications, 2017.
3. Introduction to Machine Learning, 3rd edition Adaptive Computation and Machine Learning Ethem Alpaydin, Francis Bach, series 2014.
4. Data Science: Theory, Q. A. Menon, S. A. Khoja, Analysis and Applications, CRC Press, 2020.
5. Maria Cristina Mariani, Osei Kofi Tweneboah and Maria Pia Beccar-Varela, Data Science in Theory and Practice, John Wiley and Sons publishers, 2022.

22CY355

DIGITAL WATERMARKING AND STEGANOGRAPHY

(Professional Elective-I)

Instruction	:	3 Periods/Week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Evaluation	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** To introduce essentials of watermarking models and message coding
2 **:** To get familiarity with vulnerabilities in digital watermarking
3 **:** To understand the basics of steganography

Unit–I:

Introduction- Information Hiding, Steganography and Watermarking, History of watermarking, Importance of digital watermarking, Applications, Properties, Evaluating watermarking systems.

Watermarking Models and Message Coding: Notation, Communications, Communication based models, Geometric models, Mapping messages into message vectors, Error correction coding, Detecting multi, symbol watermarks.

Unit-II:

Watermarking with side Information: Informed Embedding, Informed Coding, Structured dirty, paper codes

Analyzing Errors– Message errors: False positive errors, False negative errors, ROC curves, Effect of whitening on error rates.

Unit–III:

Perpetual Models: Evaluating perceptual impact, General form of a perceptual model, Examples of perceptual models, Robust watermarking approaches, Redundant Embedding, Spread Spectrum Coding, Embedding in Perceptually significant coefficients.

Unit–IV:

Watermark Security and Authentication: Security requirements, Watermark security and cryptography, Attacks, Exact authentication, Selective authentication, Localization, Restoration.

Unit–V:

Steganography: Steganography communication, Notation and terminology, Information theoretic foundations of steganography, Practical steganographic methods, Minimizing the embedding impact, Steganalysis.

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Familiarize the notations of Digital Watermarking techniques and compare different models available
CO 2 : Apply watermarking on digital content using the side information and analyze the error types

CO 3	:	Evaluate perpetual watermarking models on digital content
CO 4	:	Understand the types of security attacks and realize the importance of secure watermarking
CO 5	:	Familiarize the theoretical and practical aspects of steganography

Textbooks:

1. Digital Watermarking and Steganography, Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, Margan Kaufmann Publishers, New York, 2008.

References:

1. Techniques and Applications of Digital Watermarking and Contest Protection, Michael Arnold, Martin Schmucker, Stephen D. Wolthusen, Artech House, London, 2003.
2. Digital Watermarking for Digital Media, Juergen Seits, IDEA Group Publisher, New York, 2005.
3. Disappearing Cryptography – Information Hiding: Steganography & Watermarking, Peter Wayner, Morgan Kaufmann Publishers, New York, 2002.

22CY381

CYBER CRIME INVESTIGATION AND DIGITAL FORENSICS LAB

Instruction:	3 Periods/Week	Continuous Internal Evaluation	:	40 Marks
Tutorial :	-	Semester End Evaluation	:	60 Marks
Credits :	1.5	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** To provide students with a comprehensive overview of collecting, investigating, preserving, and presenting evidence of cybercrime left in digital storage devices, emails, browsers, mobile devices using different Forensics tools

2 **:** To Understand file system basics and where hidden files may lie on the disk, as well as how to extract the data and preserve it for analysis

3 **:** To understand the network analysis, Registry analysis and analyze attacks using different forensics tools and tools of e-discovery

List of Experiments

1. Perform email analysis using the tools like Exchange EDB viewer, MBOX viewer and View user mailboxes and public folders, Filter the mailbox data based on various criteria, Search for particular items in user mailboxes and public folders
2. Perform Browser history analysis and get the downloaded content, history, saved logins, searches, websites visited etc., using Foxton Forensics tool, Dumpzilla.
3. Perform mobile analysis in the form of retrieving call logs, SMS log, all contacts list using the forensics tool like SAFT
4. Perform Registry analysis and get boot time logging using process monitor tool
5. Perform Disk imaging and cloning the using the X-way Forensics tools
6. Perform Data Analysis i.e. History about open file and folder, and view folder actions using Last view activity tool
7. Perform Network analysis using the Network Miner tool.
8. Perform information for incident response using the crowd Response tool
9. Perform File type detection using Autopsy tool
10. Perform Memory capture and analysis using the Live RAM capture or any forensic tool

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Learn the importance of a systematic procedure for investigation of data found on digital storage media that might provide evidence of wrong-doing

CO 2 : To Learn the file system storage mechanisms and retrieve files in hidden format

CO 3 : Learn the use of computer forensics tools used in data analysis

CO 4 : Learn how to find data that may be clear or hidden on a computer disk, find out the open ports for the attackers through network analysis, Registry analysis

CO 5 : Learn how to detect file type memory capture and analyzing using forensic tool

Textbooks:

1. Real Digital Forensics for Handheld Devices, E. P. Dorothy, Auerback Publications, 2013.
2. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, J. Sammons, Syngress Publishing, 2012.

Reference:

1. Handbook of Digital Forensics and Investigation, E. Casey, Academic Press, 2010.
2. Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides, C. H. Malin, E. Casey and J. M. Aquilina, Syngress, 2012.
3. The Best Damn Cybercrime and Digital Forensics Book Period, J. Wiles and A.Reyes, Syngress, 2007.

22CY382

VULNERABILITY ASSESSMENT AND PENETRATION TESTING LAB

Instruction	:	3 Periods / week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	1.5	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** To develop programs using the building blocks of Security through Python API, various forensics tools
2 **:** To develop programs to solve the Network issues
3 **:** To write the code for extracting actualities by investigation software

Programs:

1. Write a Python script for finding live hosts by using the ping sweep technique.
2. Write a python program for Network Scanner.
3. Write a Python program for Simple Packet Sniffing using Scapy.
4. Write a note on various steps and practically show how to recover deleted files using forensics tools.
5. Practically show various steps for hiding and extracting any text file behind an image file/ Audio file using Command Prompt.
6. How to make the forensic image of the hard drive using EnCase Forensics?
7. How to Collect Email Evidence and Browser Artifacts in Victim PC?
8. Comparison of two Files for forensics investigation by Compare IT software.
9. Write a Python program for basic validation using Flask –Gladiator.
10. Write a python program to establish a connection between server &amp, client.
11. Write a python program to create a Forensic Image with FTK Imager.

Case Study 1: Discuss the general requirements and tools used for an Intrusion Detection System. Implement IDS in Laboratory’s network.

Case Study 2: Demonstrate “Password Strength Meter” application to measure the strength of password. Implement password cracking Techniques like Brute Force Attacks and Dictionary Attacks.

Course Outcomes: At the end of the course, the student should be able to

CO 1	:	Implement and analyze different types of API for Security
CO 2	:	Understanding various Security issues in web-based communication
CO 3	:	Develop programs to do investigation
CO 4	:	Realize the power various tools in Penetration Testing
CO 5	:	Develop a set of rules for understanding Evidence and Browser Artifacts

References:

1. Cyber Security on Azure, An IT Professional's Guide to Microsoft Azure Security Center, by Marshall Copeland, APress, 2017.

2. Cyber Security Incident Response: How to Contain, Eradicate and Recover fromIncidents, by Eric C. Thompson, Apress, USA, 2018.

22HS381/331

ADVANCED ENGLISH COMMUNICATION & SOFT SKILLS LAB
(Common to ALL)

Instruction	:	2 Periods/week	Continuous Internal Evaluation	:	40 marks
Tutorial	:	-	Semester End Examination	:	60 marks
Credits	:	1	Semester End Exam Duration	:	2 hrs

Course Objectives:

1 : To equip students with the requisite communication skills for real-time environment.
2 : To prepare students for persuasive conversations in the professional sphere.
3 : To integrate time management and decision-making skills for better performance.
4 : To modify communication to suit diverse cultures.
5 : To sensitize students to handle emotions at workplace.

Unit-I - Soft Skills & Interpersonal communication

a) Effective Communication: types of communication-verbal & non-verbal, importance of communication, 7 Cs of communication, barriers to effective communication, communication according context, strategies for improving communication.
b) Intrapersonal & Interpersonal Skills: definition, how to start a conversation, self-introduction, self-concept, signs of high & low self-esteem, self-exploration, SWOT analysis.

Unit-II - Oral Communication

a) Group Discussion- significance of GD, types of GD, opening strategies, roles of participants, evaluation parameters, dos and don’ts, types of topics, features of GD, mock GD
b) Negotiation Skills- definition, process, outcome of negotiation, skills required, strategies of communication for negotiation.
c) Book-discussion- genres of book, importance of book-discussion, purpose of book-discussion, process of book-discussion, critical and analytical skills.

Unit-III - Employability Skills

a) Team Dynamics- difference between team and group, types of teams, concepts related to team building, process of team building, roles of team player and qualities.
b) Time Management- concept of time-management, time logs, timewasters, time quadrant, priority list, tips of time management.
c) Decision-making & Problem Solving- strategies of decision-making, techniques of decision-making, problem-solving process.

Unit-IV - Cross-cultural Communication

a) Pluralism: Introduction to Cross-cultural Management, communicating across Cultures, high-low context culture, negotiating across Cultures, Motivation and Leadership across Cultures, Managing Global Teams, Global Manager
b) Diversity & adaptability- race, gender, class, caste, religion.

Unit-V - Emotional Intelligence

Concept of Emotional Intelligence: Intrapersonal Awareness, Intrapersonal Management, Conflict Management and Leadership, Anger Management

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Gain proficiency in communication skills
CO 2 : Emerge as rational speakers
CO 3 : Efficiently Manage their professional career
CO 4 : Acclimatize to diverse cultures
CO 5 : Be empowered with skills required for self-management

References:

1. Communication and Soft Skill development, Ashwini Deshpande, 1st Edition, Career Publications, 2017.
2. Effective Communication and Soft Skills, Nitin Bhatnagar and Mamta, Pearson, 2011.
3. Soft Skills & Life Skills, The Dynamics of Success, Nishitesh and Dr. Bhasker Reddi, BSC Publishers & Distributors, 2012.
4. Guide to Cross-Cultural Communications, Reynolds, Valentine and Verma, Pearson, 2010.
5. Emotional Intelligence: A Comprehensive Self Help Guide to Developing EQ, Managing Anger, and Improving your Relationships, Christopher Rance, Ingram Publishing 2019.
6. Unearthing your Emotional Intelligence, Deepa R, Notion Press, Paperback, 2020.

22HS404/451

ORGANIZATIONAL BEHAVIOUR

(Common to CSE, CSE-CS, CSE-DS and IT)

Instruction	:	3 Periods /week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 : To understand the nature, scope of Organizational Behavior along with basic concepts and its applications in contemporary organizations

2 : To deeply understand the role of personality and attitude, theories of motivation, emotional intelligence

3 : To appreciate the role and means of effective communication, decision making, strategies to reduce stress and conflict in organizations

4 : To learn about the role of power and politics, Group dynamics, Teams in the modern workplace

5 : To develop framework for high performance through leadership, job design, performance management and Quality of work life in organizations

Unit-I - Organisational Behaviour

Definition, need for and importance of organizational behaviour – Nature and scope – Frame work – Organizational behaviour models.

Unit-II - Individual Behaviour

Personality – types – Factors influencing personality – Theories – Learning – Types of learners – The learning process – Learning Theories – Organizational behaviour modification. Misbehaviour – Types – Management Intervention - Emotions – Emotional Labour – Emotional Intelligence – Theories. Attitudes – Characteristics – Components – Formation – Measurement – Values, Perceptions – Importance – Factors influencing perception – Interpersonal perception – Impression Management. Motivation – importance – Types – Effects on work behaviour.

Unit-III - Group Behaviour

Organization structure – Formation – Groups in organizations – Influence – Group dynamics -Emergence of informal leaders and working norms – Group decision making techniques – Team building – Interpersonal relations – Communication – Control.

Unit-IV - Leadership and Power

Meaning – Importance – Leadership styles – Theories of leadership – Leaders Vs Managers – Sources of power – Power centers – Power and Politics.

Unit-V - Dynamics of Organizational Behaviour

Organizational culture and climate – Factors affecting organizational climate – Importance. Job satisfaction – Determinants – Measurements – Influence on behavior. Organizational change – Importance – Stability Vs Change – Proactive Vs Reaction change - the change process - Resistance to change – Managing change. Stress– Work Stressors – Prevention and Management of stress – Balancing work and Life. Organizational development – Characteristics – objectives – Organizational effectiveness.

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Understand the nature of Organizational Behavior and its applications in an organization

CO 2 : Motivate themselves and others with a positive approach

CO 3 : Work as a team member and build a good team

CO 4 : Be good leaders

CO 5 : Work effectively in an organization

Textbooks:

1. Organizational Behavior, Luthans, Fred: 10th Edition, McGraw-Hill, 2009.
2. Organizational Behavior, Robbins, P. Stephen, 18th Edition Pearson, 2018.

References:

1. Organizational Behavior, McShane: 9th Edition, McGrawHill 2022
2. Organizational Behavior, Nelson: 3rd Edition, Thomson, 2008.
3. Organizational Behavior- Human Behavior at Work, Newstrom W. John & Davis Keith, 12th Edition, TMH, New Delhi, 2009.
4. Management and Organizational Behavior: An Integrated perspective, Pierce and Gardner, Thomson, 2009.
5. Behavioural Process at Work PareekUdai: Oxford & IBH, New Delhi, 2009.

22CY401

ETHICAL HACKING

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** The aim of the course is to introduce the methodologies and framework of ethical hacking for enhancing the security

2 **:** Learn how a cyber criminal can take advantage of security vulnerabilities.

3 **:** Learn how an individual user can become victim of cyber attacks by just clicking on any malicious link.

Unit-I

Introduction: Hacking Impacts, The Hacker.
Framework: Planning the Test Sound Operations Reconnaissance Enumeration Vulnerability Analysis Exploitation Final Analysis Deliverable Integration.
Information Security Models: Computer Security, Network Security, Service Security, Application Security, Security Architecture
Information Security Program: The Process of Information Security, Component Parts of Information, Security Programs, Risk Analysis and Ethical Hacking.

Unit-II

The Business Perspective: Business Objectives, Security Policy, Previous Test Results, Business Challenges.
Planning for a Controlled Attack: Inherent Limitations, Imposed Limitations, Timing Is Everything Attack Type Source Point Required Knowledge, Multi-Phased Attacks, Teaming and Attack Structure, Engagement Planner, The Right Security Consultant, The Tester, Logistics, Law Enforcement.

Unit-III

Preparing for a Hack: Technical Preparation, Managing the Engagement.
Reconnaissance: Social Engineering, Physical Security, Internet Reconnaissance.

Unit-IV

Enumeration: Enumeration Techniques Soft Objective Looking Around or Attack, Elements of Enumeration Preparing for the Next Phase.
Exploitation: Intuitive Testing, Evasion, Threads and Groups, Operating Systems, Password Crackers, Rootkits, Applications, Wardialing, Network Services and Areas of Concern.

Unit–V

Network Endpoint Security:
The Deliverable: The Document, Overall Structure Aligning Findings, Presentation.
Integrating the Results: Integration Summary Mitigation, Defense Planning, Incident Management, Security Policy, Conclusion.

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Gain the knowledge of the use and availability of tools to support an ethical hack

CO 2 : Discuss the business perspective of security policy and challenges

CO 3 : Understand the role of politics, inherent and imposed limitations and metrics for planning of a test.

CO 4 : Comprehend the dangers associated with penetration testing.

CO 5 : Gain the knowledge of interpreting the results of a controlled attack.

Textbooks:

1. The Ethical Hack: A Framework for Business Value Penetration Testing, James S Tiller, Auerbach Publications, CRC Press.

References:

1. Ethical Hacking and Countermeasures Attack Phases, EC-Council, Cengage Learning.
2. Hands-on Ethical Hacking and Network Defense, Micheal Simpson, Kent Backman, James Corley, Cengage Learning.

22DT402

SOFTWARE PROJECT MANAGEMENT

(Professional Elective – II)
(Common to CSE-AI&ML, CSE-CS and CSE-DS)

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Prerequisites: A course on "Software Engineering".

Course Objectives

1 **:** To develop skills in software project management
2 : To be familiar with the different methods and techniques used for project management
3 : To have a good knowledge of responsibilities of project manager

Unit-I

Conventional Software Management: The waterfall model, conventional software Management performance. Evolution of Software Economics: Software economics, pragmatic software cost estimation.

Unit-II

Improving Software Economics: Reducing Software product size, improving software processes, improving team effectiveness, improving automation, Achieving required quality, peer inspections. The old way and the new: The principles of conventional software Engineering, principles of modern software management, transitioning to an iterative process.

Unit-III

Life cycle phases: Engineering and production stages, inception, Elaboration, construction, transition phases. Artifacts of the process: The artifact sets, Management artifacts, Engineering artifacts, programmatic artifacts. Model based software architectures: A Management perspective and technical perspective. Work Flows of the process: Software process workflows, Iteration workflows.

Unit-IV

Checkpoints of the process: Major milestones, Minor Milestones, Periodic status assessments. Iterative Process Planning: work breakdown structures, planning guidelines, cost and schedule estimating, Iteration planning process, Pragmatic planning. Project Organizations and Responsibilities: Line-of-Business Organizations, Project Organizations, evolution of Organizations. Process Automation: Automation building blocks, The Project Environment.

Unit-V

Project Control and Process instrumentation: The seven core Metrics, Management indicators, quality indicators, life cycle expectations, pragmatic Software Metrics, Metrics automation. Tailoring the Process: Process discriminates. Future Software Project Management: modern Project Profiles, Next generation Software economics, modern process transitions. Case Study: The command Center Processing and Display system- Replacement (CCPDS-R).

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Explore the evaluation of software process management
CO 2 : Improve the software process architecture
CO 3 : Disseminate life cycle and workflow of the process
CO 4 : Analyse the minor and major milestones for process
CO 5 : Design the project with modern tools

Textbooks:

1. Software Project Management, Walker Royce: Pearson Education, 2005.

References:

1. Software Project Management, Bob Hughes and Mike Cotterell: Tata McGraw-Hill Edition.
2. Software Project Management, Joel Henry, Pearson Education.
3. Software Project Management in practice, Pankaj Jalote, Pearson Education. 2005.

22CY402

NETWORK MANAGEMENT SYSTEMS AND OPERATIONS

(Professional Elective – II)

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** To maintain optimal network performance and availability, and to ensure continuous uptime
2 **:** Monitor the network for problems that require special attention
3 **:** Learn various performance assessment and optimization techniques

Unit-I

The Network Management Challenge: Introduction, The Internet and Network Management, Internet Structure, Managing an Entity, Internal and External policies, The state of Network Management, Network Management in the Gartner Model, Benefits of Automation, The Lack of Industry Response, Impact on Business, Distributed Systems and new abstractions.

Unit-II

The Network Management Problem: Introduction, what is Network Management? The scope of Network Management, variety and multi-vendor environments, element and network management systems, scale and complexity, types of networks, classification of devices.

Unit–III

Configuration and Operation: Introduction, Intuition for configuration, configuration and protocol layering, dependencies among configuration parameters, seeking a more precise definition of configuration, configuration and temporal consequences, configuration and global consistency, global state and practical systems, configuration and default values, partial state, automatic update and recovery, Interface paradigm and incremental configuration, commit and rollback during configuration, automated rollback and timeout, snapshot, configuration, and partial state, separation of setup and activation.

Unit-IV

Fault detection and correction: Introduction, Network Faults, Trouble Reports, Symptoms, Causes, Troubleshooting and Diagnostics, Monitoring, Baselines, Items That Can Be Monitored, Alarms, Logs, And Polling, Identifying The Cause of a Fault, Human Failure and Network Faults, Protocol Layering and Faults, Hidden Faults and Automatic Correction, Anomaly Detection and Event Correlation, Fault Prevention.

Unit–V

Performance Assessment and Optimization: Introduction, aspects of performance, Items that can be measured, measures of network performance, application and endpoint sensitivity, degraded service, variance in traffic and congestion, congestion, delay and utilization, local and end-to-end measurements, passive observation Vs. active probing, bottlenecks and future planning, capacity Planning, planning the capacity of a switch, planning the capacity of a router, planning the capacity of an Internet connection, measuring peak and average traffic on a link, estimated peak utilization and 95th percentile, relationship between average and peak utilization, consequences for management and the 50/80 Rule, capacity planning for a complex topology, a capacity planning process, route changes and traffic engineering, failure scenarios and availability.

Course Outcomes: At the end of the course, the student should be able to

CO 1	:	Understand the basic network elements
CO 2	:	Explain various networks management problems
CO 3	:	Identify configuration and operations of network management systems
CO 4	:	Familiarize with fault detection and correction
CO 5	:	Apply various performance assessment and optimization techniques

Textbooks:

1. Automated Network Management Systems, D. Comer, Prentice Hall, 2006, ISBN No. 0132393085.
2. Nagios Core Administration Cookbook – 2nd Edition, Tom Ryder, 2016, Packt publishing, ISBN: 781785889332.
3. Terraform: Up and Running, Yevgeniy Brikman, 2017, O'Reilly Media, Inc., ISBN:9781491977088.

References:

1. Applied Network Security Monitoring, Chris Sanders, Jason Smith, Syngress publications.

22CY403

CYBER LAWS
(Professional Elective – II)

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** To make the students understand the types of roles they are expected to play in society as practitioners of the civil engineering profession
2 **:** To develop some ideas of the legal and practical aspects of their profession
3 **:** Learn how to apply the procedures and guidelines in Information Security projects

Unit–I

Introduction: History of Internet and World Wide Web, Need for cyber law, Cybercrime on the rise, Important terms related to cyber law.
Cyber law in India: Need for cyber law in India, History of cyber law in India, Information Technology Act, 2000, Overview of other laws amended by the IT Act, 2000, National Policy on Information Technology 2012.

Unit–II

Overview of The Information Technology Act, 2000: Applicability of the Act, Important provisions of the Act: Digital signature and Electronic signature, Digital Signature under the IT Act, 2000, E- Governance Attribution, Acknowledgement and Dispatch of Electronic Records, Certifying Authorities, Electronic Signature Certificates, Duties of Subscribers, Penalties and Offences, Intermediaries.

Unit–III

Overview of Rules Issued Under the It Act, 2000, Electronic Commerce, Electronic Contracts, Cyber Crimes, Cyber Frauds.

Unit–IV

Regulatory Authorities: Department of Electronics and Information Technology, Controller of Certifying Authorities (CCA), Cyber Appellate Tribuna, Indian Computer Emergency Response Team (ICERT), Cloud Computing, Case Laws.

Unit–V

Introduction to Cybercrime and Procedure To Report Cybercrime: Procedure To Report Cyber Crime, Some Basic Rules For Safe Operations Of The Computer And Internet, The Criminal Law (Amendment) Act, 2013: Legislative Remedies For Online Harassment And Cyberstalking In India.

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Assimilate the vocabulary of information security laws and familiarize the policy sets
CO 2 : Familiarize various Information security policies, standards and guidelines
CO 3 : Compare and contrast various frameworks on Information Security
CO 4 : Realize the structure legal language of Information Security procedures
CO 5 : Apply the procedures and guidelines in Information Security projects

Textbooks:

1. Textbook on Cyber Law, Pavan Duggal, 2nd Edition, Universal Law.
2. Indian Cyberlaw on Cyber Crimes, Pavan Duggal.

References:

1. Computer Security Basics (Paperback), Debby Russell and Sr. G.T. Gangemi, 2nd Edition, O’ Reilly Media, 2006.
2. Information Security policies and procedures: Thomas R. Peltier, A Practitioner’s Reference, 2nd Edition Prentice Hall, 2004.
3. Cyber Security and Global Information Assurance: Kenneth J. Knapp, Threat Analysis and Response Solutions, IGI Global, 2009.
4. Information Security Fundamentals, Thomas R Peltier, Justin Peltier and John blackley, 2nd Edition, Prentice Hall, 1996.

22CY404/356

BIOMETRICS FOR SECURITY
(Professional Elective-II)
(Common to CSE-CS AND IT)

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives

1 **:** To Understand Biometric Fundamentals, comprehensive Knowledge of Finger Biometric Technology and Facial Biometric Technology
2 **:** To mastery of Iris and Voice Biometric Technologies
3 **:** Exploration of Physiological and Behavioral Biometrics

Unit-I Introduction

Benefits of biometrics, Verification and identification: Basic working of biometric matching, Accuracy, False match rate, False non-match rate, Failure to enroll rate, Active and passive biometric, Parameters of a good biometrics.

Unit-II

Finger Biometric Technology: General description of fingerprints, Micro and Macro Features, Types of algorithms used for interpretation, Components and Operations: Strength and weakness.

Facial Biometric Technology: General description, Features, Types of algorithms used for interpretation, Components and Operations, Strength and weakness.

Unit-III

Iris Biometric Technology: General description, Feature, Mechanism of iris recognition, Components and Operations, Strength and weakness.

Unit-IV

Voice Biometric Technology: General description, Feature, Types of algorithms used for interpretation, Components and Operations, Strength and weakness.

Unit-V

Physiological Biometrics: Hand scan, Retina scan, Behavioral Biometrics: Signature scan, keystroke scan etc.

Course Outcomes: At the end of the course, the student should be able to

CO1 : Understand the advantages of employing biometrics in various applications, including security, identification, and access control
CO2 : Comprehensive grasp of fingerprints and facial biometrics include features, algorithms, and applications for accurate interpretation
CO3 : Master iris biometrics include technology, features, algorithms for accurate interpretation and application in various contexts
CO4 : Integrate diverse biometric modalities for enhanced security and identification across voice, physiology, and behavior
CO5 : Understand and apply biometric techniques for secure identity verification and access control in diverse physiological and behavioral modalities

Textbooks:

1. Biometrics for Network Security, Reid Paul, Pearson,2003.
2. Biometrics, Woodward, J.D. and Orlans, Nicholos M., McGraw Hill, 2002.

References:

1. Biometrics: Concepts and Applications, G R Sinha and Sandeep B. Patil, Wiely, 2013
2. Biometrics- Identity verification in a network, Samir Nanavathi, Michel Thieme and Raj Nanavathi, Wiley Eastern, 2002.

22IT403

QUANTUM COMPUTING

(Professional Elective-III)
(Common to IT, CSE, CSE-AI&ML, CSE-CS AND CSE-DS)

Instruction	:	3 Periods / week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Prerequisites: A course on "Data Structures"

Course Objectives:

1 : To Understand the basic Concepts of Linear Algebra related to Quantum Computing
2 : To Master the basics of physics-oriented phenomenon related to Quantum Computing
3 : To get familiar with various Quantum Architecture and Quantum Algebra

Unit–I

Introduction to Essential Linear Algebra: Some Basic Algebra, Matrix Math, Vectors and Vector Spaces, Set Theory. Complex Numbers: Definition of Complex Numbers, Algebra of Complex Numbers, Complex Numbers Graphically, Vector Representations of Complex Numbers, Pauli Matrice, Transcendental Numbers. Database System, The Journey to Quantum Computing.

Unit–II

Basic Physics for Quantum Computing: Quantum Physics Essentials, Basic Atomic Structure, Hilbert Spaces, Uncertainty, Quantum States, Entanglement. **Basic Quantum Theory:** Further with Quantum Mechanics, Quantum Decoherence, Quantum Electrodynamics, Quantum Chromodynamics, Feynman Diagram Quantum Entanglement and QKD, Quantum Entanglement, Interpretation, QKE.

Unit-III

Quantum Architecture: Further with Qubits, Quantum Gates, More with Gates, Quantum Circuits, The D-Wave Quantum Architecture. Quantum Hardware: Qubits, How Many Qubits Are Needed? Addressing Decoherence, Topological Quantum Computing, Quantum Essentials. Introduction to Query Language

Unit–IV

Quantum Algorithms: Introduction, Deutsch's Algorithm, Deutsch-Jozsa Algorithm, Bernstein-Vazirani Algorithm, Simon's Algorithm, Shor's Algorithm, Grover's Algorithm

Unit–V

Current Asymmetric Algorithms: RSA, Diffie-Hellman, Elliptic Curve. The Impact of Quantum Computing on Cryptography: Asymmetric Cryptography, Specific Algorithms, Specific Applications.

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Understand basics of quantum computing
CO 2 : Understand physical implementation of Qubit
CO 3 : Understand Quantum algorithms and their implementation
CO 4 : Understand the Impact of Quantum Algorithms and its significance
CO 5 : Realize the importance of current Asymmetric Algorithms on Quantum computing

Textbooks:

1. Quantum Computation and Quantum Information, Nielsen M. A., Cambridge University Press.
2. Quantum Computing Fundamentals, Dr. Chuck Easttom, Pearson.

References:

1. Quantum Computing for Computer Scientists by Noson S. Yanofsky and Mirco A. Mannucci
2. Principles of Quantum Computation and Information, Vol, Benenti G., Casati G. and Strini G.
3. Basic Concepts. Vol. Basic Tools and Special Topics, World Scientific.
4. An Introduction to Quantum Computing Algorithms, Pittenger A. O.

22CY405

BLOCKCHAIN TECHNOLOGIES

(Professional Elective-III)
(Common to CSE-CS, CSE AND IT)

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** Conceptual understanding of the function of Blockchains as a method of securing distributed ledgers, how consensus on their contents is achieved

2 **:** To understand blockchain operations as distributed data structures and decision-making systems

3 **:** To evaluate "smart contract" capabilities and platforms, and examines their future directions, opportunities, risks, and challenges

Unit–I:

Introduction to Blockchain: The growth of Block chain technology, Distributed systems, History of Blockchain and Bitcoin, Types of Block chain, Consensus, CAP theorem and Blockchain**.**
Decentralization: Decentralization using block chain, Methods of decentralization, Routes to decentralization, Blockchain and full ecosystem decentralization, Smart contracts, Decentralized Organizations, Platforms for decentralization.

Unit–II:

Bitcoins: Introducing Bitcoin, Digital keys and addresses, Transactions**,** the structure of a block, Mining. **Bitcoin Network and Payments:** The Bit coin network, Wallets, Bitcoin payments: Innovation in Bitcoin, Bitcoin Clients, and APIs, Bit coin installation, Alternative Coins, Bitcoin limitations.

Unit–III:

Smart Contracts: History, Definition, Ricardian contracts, Introduction to Ethereum, Components of the Ethereum ecosystem, Further Ethereum, Programming languages.

Unit–IV:

Ethereum Development Environment: Test networks, Development Tools and Frameworks, Compilers, Solidity compiler (solc), Integrated Development Environments (IDEs).
Solidity language: Layout of a Solidity, Data Types: Reference types, Value types; Literals, Enums, Function types, Global variables, Control structures.

Unit–V:

Hyperledger: Projects under Hyperledger, Hyperledger as a protocol, the reference architecture, Requirements and design goals of Hyperledger Fabric, Hyperledger Fabric, Membership services, Blockchain services, Consensus services, Distributed ledger.
Beyond Cryptocurrency: Applications of blockchain in cyber security, integrity of information, E-Governance and other contract enforcement mechanisms, Limitations of blockchain as a technology, and myths vs. reality of blockchain technology.

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Understand the structure of a blockchain and how it is better than a simple distributed database

CO 2 : Evaluate the blockchain based structure along with its potentials and its limitations

CO 3 : Understand smart‖ contract and what are its legal implications and what it can and cannot do

CO 4 : Attain awareness of the new challenges around blockchains and smart contracts

CO 5 : Understand the differences between the different blockchain structures and their specific uses

Textbooks:

1. Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more, 3rd Edition, Imran Bashir, Packt Publishing, 2020.
2. Mastering Blockchain, Imran Bashir, 2nd Edition, Packt Publishing, March 2018.
3. Mastering Bitcoin Programming the Open Blockchain, Andreas M. Antonopoulos, 2nd Edition, O'Reilly Media, Inc., June 2017.

References:

1. Hyperledger Fabric - https://www.hyperledger.org/projects/fabric.
2. Hyperledger Tutorials - https://www.hyperledger.org/use/tutorials
3. Ethereum Development Resources - https://ethereum.org/en/developers

22IT404

CLOUD SECURITY

(Professional Elective-III)

(Common to IT, CSE AND CSE-CS)

Instruction	:	3 Periods / week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Prerequisites: Fundamentals of cyber security

Course Objectives:

1 **:** Fundamentals of cloud computing architectures based on current standards, SLA, and cloud security models to integrate.
2 **:** Understand the industry security standards, regulatory mandates, audit policies and compliance requirements for Cloud based infrastructures.
3 **:** Approaches to designing cloud services that meets essential Cloud infrastructure security and management.
4 **:** Identify the known threats, risks, vulnerabilities, and privacy issues associated with Cloud based IT services and IAM services.

Unit–I

Cloud Computing Architectural Framework: Cloud Computing Evolution, Essential Characteristics of Cloud Computing, Cloud Deployment Architecture, Cloud Deployment models, Cloud Service Models, SLA.
Introduction to Cloud Security: Introduction, Cloud Security Concepts, Cloud security Standards, CSA Cloud Reference Model, NIST Cloud Reference model.

Unit-II

Compliance and Audit: Cloud customer responsibilities, Compliance and Audit Security Recommendations. Portability and Interoperability: Changing providers reasons, Changing providers expectations, Internal Policy compliance, governance risk compliance(GRC),
Cloud Security and Privacy Issues: Introduction, Cloud Security Goals/Concepts, Cloud Security Issues, Security Requirements for Privacy, Privacy Issues in Cloud.

Unit-III

Cloud Infrastructure Security: Identity and Access Management (IAM) in cloud environments, Virtual Private Cloud (VPC) and network security, Secure provisioning and configuration management in the cloud. The Network Level, the Host Level, the Application Level. Security Management In Cloud, Availability management for SAAS, PAAS, IAAS.

Unit-IV

Threat Model and Cloud Attacks: Introduction, Threat Model- Type of attack entities, Attack surfaces
with attack scenarios, A Taxonomy of Attacks, Attack Tools-Network-level attack tools, VM-level attack tools, VMM attack tools, Security Tools, VMM security tools

Unit-V

Identity and Access Management: The role of IAM in cloud security, Key concepts: authentication, authorization, and auditing, oAuth and SSO, User identity and access lifecycle management, Configuring IAM in cloud platforms (e.g., AWS, Azure). **Authorization and Role-Based Access Control (RBAC)** Role-based access control principles, Creating and managing roles in cloud platforms, Least privilege principle.
Identity Federation- Understanding identity federation, Cross-domain and cross-cloud identity integration, Use cases and challenges, Virtualization, Virtualization Security Recommendations.

Course Outcomes: At the end of the course, the student should be able to

CO 1	:	Demonstrate the growth of Cloud computing and cloud security, architecture, and different modules of implementation
CO 2	:	Evaluate the different types of cloud Compliance and Audit, Security and Privacy Issues
CO 3	:	Access the security implementation flow, actions and responsibilities of stake holders using IAM
CO 4	:	Analyse the various threats and Attack tools details
CO 5	:	Implement based on roles and groups policy created and choose the type of virtualization to be used

Textbooks:

1. Cloud Security and Privacy, An Enterprise Perspective on Risks and Compliance by Tim Mather, Subra Kumaraswamy, Shahed Latif, Oreilly Media, 2009.
2. Cloud Security Attacks, Techniques, Tools, and Challenges by Preeti Mishra, Emmanuel S Pilli, Jaipur R C Joshi Graphic Era, 1st Edition published 2022 by CRC press.

Reference:

1. Securing the Cloud, Cloud Computer Security Techniques and Tactics by Vic (J.R.) Winkler, Syngress, 2011.
2. Online documentation and tutorials from cloud service providers (e.g., AWS, Azure, GCP)

22CY406

AUTHENTICATION TECHNIQUES

(Professional Elective-III)

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** Knowledge on concept of authentication types, protocols, physical identification and various authentication algorithms
2 **:** Learn text based and voice-based authentication techniques
3 **:** Learn how to apply various authentication protocols in multi-server environment

Unit-I:

Definition of Authentication, Identification/verification, Stages and steps of authentication, Authentication Entity: User, Device and Application; Authentication attributes: Source, Location, Path, Time duration etc.; Authentication Types : Direct / Indirect, One Way / Mutual, On demand/ Periodic/Dynamic/Continuous authentication, Assisted/Automatic; 3 Factors of authentication; Passwords, Generation of passwords of varied length and of mixed type, OTP, passwords generation using entity identity credentials; Secure capture, processing, storage, verification and retrieval of passwords.

Unit-II:

Physical identification using smart cards, remote control device, proximity sensors, surveillance camera, authentication in Card present / Card Not Present transactions as ATM/ PoS Device, mobile phone, wearable device and IoT device-based authentication; single sign- on; Symmetric Key Generation, Key Establishment, Key Agreement Protocols.

Unit-III:

Biometrics – photo, face, iris, retinal, handwriting, signature, fingerprint, palm print, hand geometry, voice – Text based and text independent voice authentication, style of talking, walking, writing, keystrokes, gait etc. multi-modal biometrics.

Unit-IV:

Matching algorithms, Patterns analysis, errors, performance measures, ROC Curve; Authentication Standards – International, UIDAI Standard. Kerberos, X.509 Authentication Service, Public Key Infrastructure, Scanners and Software; Web Authentication Methods: Http based, Token Based, OAuthand API.

Unit-V:

User authentication protocols in multi-server environment, BAN Logic, Representation of authentication protocols using BAN Logic, Random Oracle Model, Scyther Tools, Proverif tool, Chebyshev Chaotic Map, Fuzzy Extractor, Fuzzy Extractor Map, Bloom Filter, LU Decomposition based User Authentication, Blockchain based authentication.

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Understand different types of authentication techniques
CO 2 : Understand text based and voice-based authentication techniques
CO 3 : Understand significance of authentication algorithms and its standards
CO 4 : Perform risk management, controlling application privacy from social media
CO 5 : Apply various authentication protocols in multi-server environment and their representation

Textbooks:

1. Protocols for Authentication and Key Establishment, Colin Boyd and Anish Mathuria, springer, 2021
2. Guide to Biometrics, Ruud M.Bolle, Sharath Pankanti, Nalini K. Ratha, Andrew W. Senior, Jonathan H.Connell, Springer 2009.

References:

1. Digital Image Processing using MATLAB, Rafael C. Gonzalez, Richard Eugene Woods, 2nd Edition, Tata McGraw-Hill Education 2010.
2. Biometric System and Data Analysis: Design, Evaluation, and data Mining, Ted Dunstone and Neil Yager, Springer.
3. Biometrics Technologies and verification Systems, John Vacca, Elsevier Inc., 2007.
4. Pattern Classification, Richard O. Duda, David G.Stork,Peter E. Hart, Wiley 2007.

22DT434/382

BIG DATA ANALYTICS LAB

(Common to CSE-CS AND CSE-DS)

Instruction	:	2 Periods / week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	1	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 : Understand big data for business intelligence. Learn business case studies for big data analytics

2 : Understand NoSQL big data management. Perform map-reduce analytics using Hadoop and related tools

Exercises:

1. Revise programs on java
2. Implement the following file management tasks in Hadoop:

   o Adding files and directories
   o Retrieving files
   o Deleting files

   Hint: A typical Hadoop workflow creates data files (such as log files) elsewhere and copies them into HDFS using one of the above command line utilities.

2. Run a basic Word Count Map Reduce program to understand Map Reduce Paradigm.
3. Write a Map Reduce program that mines weather data.

   Gather a large volume of log data from Weather sensors every hour from many locations across the globe, which is a good candidate for analysis with MapReduce, since it is semi structured and record-oriented.

4. Implement Matrix Multiplication with Hadoop Map Reduce
5. Install and Run Pig, write Pig Latin scripts to sort, group, join, project, and filter your data.
6. Install and Run Hive, use Hive to create, alter, and drop databases, tables, views, functions, and indexes
7. Write a JDBC Program to create a HIVE database EMPLOYEE table with the attributes empname, salary, age, joining date, address.
8. Write a JDBC program to perform join operations on EMPLOYEE and SALARY table using PIG operators.
9. Illustrate the PIG string functions and date and time functions with student database.
10. Installing MongoDB. Illustrate the following – inserting, finding and querying data, importing data.

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Install Hadoop and perform basic file management task
CO 2 : Implement basic data structures in Hadoop
CO 3 : Apply map reduce technique to solve various problems
CO 4 : Install Pig and Hive and execute to do basic programs
CO 5 : Install MongoDB and do basic programs.

Text Books:

1. Big Data and Hadoop, V.K. Jain, Khanna Book Publishing, Delhi.
2. Hadoop: The Definitive Guide, Tom White, 3rd Edition, O'Reilly, 2012.

References:

1. Big Data, Big Analytics: Emerging Business Intelligence and Analytic Trends for Today's Businesses, Michael Minelli, Michelle Chambers, and AmbigaDhiraj, Wiley, 2013.

22CY431

ETHICAL HACKING LAB

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	1.5	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** The aim of the course is to introduce the methodologies framework tools of ethical hacking to get awareness in enhancing the security

2 **:** To get knowledge on various attacks and their detection

List of Experiments:

1. Setup a honey pot and monitor the honey pot on network.
2. Write a script or code to demonstrate SQL injection attacks.
3. Create a social networking website login page using phishing techniques.
4. Write a code to demonstrate DoS attacks.
5. Install rootkits and study variety of options.
6. Study of Techniques uses for Web Based Password Capturing.
7. Install jcrypt tool (or any other equivalent) and demonstrate Asymmetric, Symmetric Crypto algorithm, Hash and Digital/PKI signatures studied in theory Network Security and Management
8. Implement Passive scanning, active scanning, session hijacking, cookies extraction using Burp suit tool

Course Outcomes: At the end of the course, the student should be able to

CO 1	:	Explore the technique to set up Intrusion Detection System
CO 2	:	Demonstrate techniques of Social Engineering attack
CO 3	:	Gain the knowledge of the use and availability of tools to support an ethical hack
CO 4	:	Interpret the results of controlled attacks in ethical hack
CO 5	:	Illustrate the tool to identify Network Vulnerabilities

Textbooks:

1. Hands-on Ethical Hacking and Network Defense by James Corley, Kent Backman, and Michael Simpson, Third Edition, Course Technology, CENGAGE LEARNING.
2. EC-Council, Ethical Hacking and Countermeasures Attack Phases, Cengage Learning.

22CY451

DATA ANALYTICS FOR FRAUD DETECTION

(Professional Elective-IV)

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

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

Unit-I:

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

Unit-II:

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

Unit-III:

Data Analytical Tests: Benford's Law, Number Duplication Test, Z-Score, Relative Size Factor Test, Same-Same-Same Test, Same-Same-Different Test.

Unit-IV:

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

Unit-V:

Payroll Fraud, Expense Reimbursement Schemes, Register disbursement schemes.

Course Outcomes: At the end of the course, the student should be able to

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

Textbooks:

1. Fraud and Fraud Detection: A Data Analytics Approach by Sunder Gee, Wiley.

References:

1. Data analysis techniques for fraud detection, Blokdyk Gerardus, CreateSpace Independent Publishing Platform.
2. Fraud Data Analytics Methodology: The Fraud Scenario Approach to Uncovering Fraud in Core Business Systems, Leonard W. Vona, Wiley.

22CY452

5G TECHNOLOGIES
(Professional Elective –IV)

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** Knowledge on the concepts of 5G and 5G technology drivers
2 **:** Understand 5Gnetwork architecture, components, features and their benefits
3 **:** Learn and analyze Device-to-device(D2D) and machine-to-machine(M2M) type communications

Unit-I

Over view of 5G Broad Band Wireless Communications: Evolution of mobile technologies 1G to 4G (LTE, LTEA, LTEA Pro), An Overview of 5G requirements, Regulations for 5G, Spectrum Analysis and Sharing for 5G.

Unit-II

The 5G wireless Propagation Channels: Channel modeling requirements, propagation scenarios and challenges in the 5G modeling, Channel Models for mm Wave MIMO Systems, 3GPP standards for 5G.

Unit-III

Transmission and Design Techniques for 5G: Basic requirements of transmission over 5G, Modulation Techniques, Orthogonal frequency division multiplexing (OFDM), generalized frequency division multiplexing (GFDM), filter bank multi-carriers (FBMC) and universal filtered multi-carrier (UFMC), Multiple Accesses Techniques, orthogonal frequency division multiple accesses(OFDMA), generalized frequency division multiple accesses(GFDMA), non-orthogonal multiple accesses(NOMA).

Unit-IV

Device-to-device (D2D) and machine-to-machine (M2M) type communications, Extension of 4G D2D standardization to 5G, radio resource management for mobile broadband D2D, multi-hop and multi-operator D2D communications.

Unit-V

Millimeter-wave Communications, spectrum regulations, deployment scenarios, beam-forming, physical layer techniques, interference and mobility management, Massive MIMO propagation channel models, Channel Estimation in Massive MIMO, Massive MIMO with Imperfect CSI, Multi-Cell Massive MIMO, Pilot Contamination, Spatial Modulation(SM).

Course Outcomes: At the end of the course, the student should be able to

CO 1	:	Understand 5G and 5G Broadband Wireless Communications
CO 2	:	Understand 5G wireless Propagation Channels
CO 3	:	Understand the significance of transmission and Design Techniques for 5G
CO 4	:	Analyze Device-to-device(D2D) and machine-to-machine(M2M) type communications
CO 5	:	Learn Massive MIMO propagation channel models

Textbooks:

1. From GSM from GSM to LTE Advanced Pro and 5G: An Introduction to Mobile Networks and Mobile Broadband, Martin Sauter, Wiley-Blackwell.
2. Fundamentals of 5G Mobile Networks, AfifOsseiran, Jose. F.Monserrat, PatrickMarsch, Cambridge University Press.

References:

1. Fundamentalsof5GMobileNetworks, Jonathan Rodriguez, JohnWiley & Sons.
2. Essentials of LTE and LTE-A, Amitabha Ghosh and Rapeepat Ratasuk, Cambridge University Press.
3. New Directions in Wireless Communication Systems from Mobile to 5G, Athanasios G.Kanatos, Konstantina S.Nikita, Panagiotis Mathiopoulos, CRC Press.
4. Millimeter Wave Wireless Communications, Theodore S.Rappaport, RobertW.Heath, Robert C.Danials, JamesN. Murdock, Prentice Hall Communications.

22CY453

WEB SECURITY

(Professional Elective – IV)

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** Give an Overview of information security
2 **:** Give an overview of Access control of relational databases
3 **:** Learn and understand client-side and server-side programming

Unit-I

The Web Security, The Web Security Problem, Risk Analysis and Best Practices Cryptography and the Web, Cryptography and Web Security, Working Cryptographic Systems and Protocols, Legal Restrictions on Cryptography, Digital Identification

Unit-II

The Web's War on Your Privacy, Privacy-Protecting Techniques, Backups and Antitheft, Web Server Security, Physical Security for Servers, Host Security for Servers, Securing Web Applications

Unit-III

Database Security: Recent Advances in Access Control, Access Control Models for XML, Database Issues in Trust Management and Trust Negotiation, Security in Data Warehouses and OLAP Systems

Unit-IV

Security Re-engineering for Databases: Concepts and Techniques, Database Watermarking for Copyright Protection, Trustworthy Records Retention, Damage Quarantine and Recovery in Data Processing Systems, Hippocratic Databases: Current Capabilities.

Unit-V

Future Trends Privacy in Database Publishing: A Bayesian Perspective, Privacy-enhanced Location-based Access Control, Efficiently Enforcing the Security and Privacy Policies in a Mobile Environment

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Understand the Web architecture and applications
CO 2 : Understand client-side and server-side programming
CO 3 : Understand how common mistakes can be bypassed and exploit the application
CO 4 : Understand the importance of securing the data and the techniques to secure it
CO 5 : Identify common application vulnerabilities

Textbooks:

1. Web Security, Privacy and Commerce Simson GArfinkel, Gene Spafford, O'Reilly.
2. Handbook on Database security applications and trends Michael Gertz, Sushil Jajodia.

References:

1. Web Application Security: Exploitation and Countermeasures for Modern Web Applications, Andrew Hoffman, O'reilly.
2. Identity and Data Security for Web Development - Best Practices, Jonathan LeBlanc Tim Messerschmidt, O'reilly.
3. Web Security for Developers, McDonald Malcolm, No Starch Press, US.

22CY454

DATABASE SECURITY

(Professional Elective-IV)
(Common to CSE-CS and CSE-DS)

Instruction	:	3 Periods / week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** To learn the security of databases
2 **:** To learn the design techniques of database security
3 **:** To learn the secure software design

Unit-I

Introduction: Introduction to Databases Security Problems in Databases Security Controls Conclusions
Security Models -1: Introduction Access Matrix Model, Take-Grant Model, Acten Model, PN Model Hartson and Hsiao's Model Fernandez's Model Bussolati and Martella's Model for Distributed databases.

Unit-II

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

Unit-III

Security Software Design: Introduction, A Methodological Approach to Security Software Design Secure Operating System Design, Secure DBMS Design Security Packages Database Security Design 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.

Unit-IV

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.

Unit-V

Models for the Protection of New Generation Database Systems -2: A Model for the Protection of New Generation Database Systems, The Orion Model, Ajodia and Kogan's Model, A Model for the Protection of Active Databases, Conclusions.

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Ability to carry out a risk analysis for large database
CO 2 : Ability to set up, and maintain the accounts with privileges and roles
CO 3 : Gaining knowledge on security software design, database protection & intrusion detection systems
CO 4 : Understanding different protection models related to databases like Object oriented, Relational etc.,
CO 5 : Ability to understand the protection of new generation databases

Textbooks:

1. Database Security by Castano, Pearson Edition.
2. Database Security and Auditing: Protecting Data Integrity and Accessibility, 1st Edition, Hassan Afyouni, THOMSON Edition.

References:

1. Database security by Alfred basta, melissazgola, CENGAGE learning.

22IT451

DESIGN PATTERNS

(Professional Elective-V)

(Common to IT, CSE, CSE-AI&ML, CSE-CS AND CSE-DS)

Instruction	:	3 Periods / week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Prerequisites:

1. Object Oriented Programming through Java
2. Software Engineering

Course Objectives:

1 **:** To make the students understand the basic concepts of Design patterns.
2 **:** To understand the various Design patterns.
3 **:** To understand the importance of design patterns for development of a reusable product.

Unit-I – Introduction

Introduction: What Is a Design Pattern? Design Patterns in Smalltalk MVC, Describing Design Patterns, The Catalog of Design Patterns, Organizing the Catalog, How Design Patterns Solve Design Problems, How to Select a Design Pattern, How to Use a Design Pattern.

Unit-II – A Case Study

A Case Study: Designing a Document Editor: Design Problems, Document Structure, Formatting, Embellishing the User Interface, Supporting Multiple Look-and-Feel Standards, Supporting Multiple Window Systems, User Operations Spelling Checking and Hyphenation, Summary What to Expect from Design Patterns.

Unit-III – Creational Patterns

Creational Patterns: Abstract Factory, Builder, Factory Method, Prototype, Singleton, Discussion of Creational Patterns.

Unit-IV – Structural Patterns

Structural Patterns: Adapter, Bridge and Composite, Decorator, façade, Flyweight, Proxy.

Unit-V – Behavioral Patterns

Behavioral Patterns: Chain of Responsibility, Command, Interpreter, Iterator, Mediator, Memento, Observer, State, Strategy, Template Method, Visitor, Discussion of Behavioral Patterns.

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Appreciate the basic concepts of design patterns and able to know how to select and use the design patterns
CO 2 : Identify the design pattern in the existing code and use of creational patterns
CO 3 : Apply and use the structural patterns
CO 4 : Identify and use the behavioral patterns
CO 5 : Find and catalog patterns in the object-oriented software

Textbooks:

1. Design Patterns: Elements of Reusable Object-Oriented Software, Erich Gamma, Richard Helm, Ralph Johnson and John Vlissides, Addison-Wesley, 1995.
2. Java™ Design Patterns: A Tutorial, James W. Cooper, Addison Wesley, 2000.

References:

1. Patterns in Java: A Catalog of Reusable Design Patterns Illustrated with UML, Mark Grand, Volume 2, Wiley DreamTech.
2. Patterns in Java, Mark Grand, Volume 2, Wiley DreamTech, 2008.
3. Java Enterprise Design Patterns, Mark Grand, Wiley DreamTech, 2006.

22CY455

CYBER FORENSICS

(Professional Elective-V)
(Common to CSE-CS AND CSE)

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** A brief explanation of the objective is to provide digital evidences which are obtained from digital media.

2 **:** In order to understand the objectives of computer forensics, first of all, people have to recognize the different roles computer plays in a certain crime.

3 **:** According to a snippet from the United States Security Service, the functions computer has in different kinds of crimes.

Unit-I

Introduction of Cybercrime: Types, The Internet spawn's crime, Worms versus viruses, Computers roles in crimes, Introduction to digital forensics, Introduction to Incident - Incident Response Methodology, Steps, Activities in Initial Response, Phase after detection of an incident.

Unit-II

Initial Response and forensic duplication, Initial Response & Volatile Data Collection from Windows system, Initial Response & Volatile Data Collection from Unix system
Forensic Duplication: Forensic duplication, Forensic Duplicates as Admissible Evidence, Forensic Duplication Tool Requirements, Creating a Forensic. Duplicate/Qualified Forensic, Duplicate of a Hard Drive.

Unit-III

Forensics analysis and validation: Determining what data to collect and analyze, validating forensic data, addressing data-hiding techniques, performing remote acquisitions.
Network Forensics: Network forensics overview, performing live acquisitions, developing standard procedures for network forensics using network tools, examining the honeynet project.

Unit-IV

Current Forensic tools: evaluating computer forensic tool needs, computer forensics software tools, computer forensics hardware tools, validating and testing forensics software.
E-Mail Investigations: Exploring the role of e-mail in investigation, exploring the roles of the client and server in e-mail, investigating e-mail crimes and violations, understanding e-mail servers, using specialized e-mail forensic tools.
Cell phone and mobile device forensics: Understanding mobile device forensics, understanding acquisition procedures for cell phones and mobile devices.

Unit-V

Working with Windows and DOS Systems: understanding file systems, exploring Microsoft File Structures, Examining NTFS disks, Understanding whole disk encryption, windows registry, Microsoft startup tasks, MS-DOS startup tasks, virtual machines.

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Familiarize Various Cybercrime types
CO 2 : Explain Initial Response and data collection from various system
CO 3 : Analyze and validate forensic data and develop standard procedures for network forensics
CO 4 : Use various forensic tools for a wide variety of investigations
CO 5 : Examine File Systems and disk encryption

Textbooks:

1. Incident Response and computer forensics, Kevin Mandia, Chris Prosise, Tata McGraw Hill, 2006.
2. Computer Forensics, Computer Crime Investigation by John R. Vacca, Firewall Media, New Delhi.
3. Computer Forensics and Investigations by Nelson, Phillips Enfinger, Steuart, CENGAGE Learning.

References:

1. Real Digital Forensics by Keith J. Jones, Richard Bejtiich, Curtis W. Rose, Addison- Wesley Pearson Education
2. Forensic Compiling, A Tractitioneris Guide by Tony Sammes and Brian Jenkinson, Springer International edition.

22CY456

SOCIAL MEDIA SECURITY

(Professional Elective-V)

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** To understand types, values and opportunities of social media
2 **:** To demonstrate the various consideration for setting up and promotion of social media
3 **:** To discuss the risk and dark side of social media

Unit-I:

Introduction to Social Media: Understanding Social Media, Different Types and Classifications, The Value of Social Media, Cutting Edge Versus Bleeding Edge, The Problems That Come with Social Media, Is Security Really an Issue? Taking the Good with the Bad.
Opportunities of Social Media: Opportunities of Social Media, New Methods of Marketing to Customers, Building Social Authority, Engaging Customers, Sharing Information, Getting The Word Out, Taking Advantage of Collective Intelligence.

Unit-II:

Considerations for setting up Social Media: Identifying How Social Media will be used in Your Organization, Identifying Your Audience, Internet Versus Intranet, Making the Right Decisions Early, Identifying How You'll Represent Yourself on the Internet, Approved Representatives, Privacy, Training and Policy.
Being Bold Versus Being Overlooked: Being bold versus being overlooked, Good social media campaigns, Bad social media campaigns, sometimes it's better to be overlooked, Social media hoaxes, The human factor, Content management, Promotion of social media.

Unit-III:

Risks of Social Media: Risks of social media, Public embarrassment, Once it's out there, it's out there, False information, Information leakage, Retention and archiving, Loss of data and equipment.
The Dark Side: Cybercrime, Social engineering, Hacked accounts.

Unit-IV:

Risk Management: Laws and regulations, Insurance, Forensics, Police use of social media, Malware, viruses, and exploit distribution.
Policies and Privacy: Policies, Privacy, Blocking users, Controlling app privacy, Location awareness.

Unit-V:

Security: Security, Fake accounts, Passwords, Privacy and information sharing, Content security.

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Familiarize various characteristics and types of social media
CO 2 : Gain knowledge on considerations for setting up social media
CO 3 : Able to identify the risks and dark side of social media
CO 4 : Perform risk management, controlling application privacy from social media
CO 5 : Learn different parts of social media security

Textbooks:

1. Social Media Security- Leveraging Social Networking While Mitigating Risk, Michael Cross, Syngress publications, 2014.

References:

1. Using Social Media for Global Security, Ravi Gupta, Hugh Brooks, Wiley Publications, 2013.

22DT455

INFORMATION STORAGE MANAGEMENT

(Professional Elective – V)

(Common to CSE-CS AND CSE-DS)

Instruction	:	3 Periods/week	Continuous Internal Evaluation	:	40 Marks
Tutorial	:	-	Semester End Examination	:	60 Marks
Credits	:	3	Semester End Exam Duration	:	3 Hours

Course Objectives:

1 **:** To understand the basic components of Storage System Environment
2 **:** To understand the Storage Area Network Characteristics and Components
3 **:** To describe the different backup and recovery topologies

Unit–I:

Introduction to Storage Technology: Data proliferation and the varying value of data with time & usage, Sources of data and states of data creation, Overview of basic storage management skills and activities, The five pillars of technology, Overview of storage infrastructure components, Evolution of storage, Information Lifecycle Management concept, Data categorization within an enterprise, Storage and Regulations.

Unit–II:

Storage Systems Architecture: Intelligent disk subsystems overview, Contrast of integrated vs. Modular arrays, Component architecture of intelligent disk subsystems, Disk physical structure components, properties, performance, and specifications, Logical partitioning of disks, RAID & parity algorithms, hot sparing, Physical vs. logical disk organization, protection, and back end management, Array caching properties and algorithms, Front end connectivity and queuing properties, Front end to host storage provisioning, mapping, and operation, Interaction of file systems with storage, Storage system connectivity protocols.

Unit–III:

Introduction to Networked Storage: JBOD (Just a Bunch of Disks), DAS, SAN, NAS, & CAS evolution. Direct Attached Storage (DAS) – elements, connectivity, and management. Storage Area Networks (SAN) - elements and connectivity, Fibre Channel principles, standards, network management principles. Network Attached Storage (NAS): elements, connectivity options, connectivity protocols (NFS, CIFS, ftp), management principles, standards (iSCSI, FCIP, iFCP). Content Addressable Storage (CAS): elements, connectivity options, standards, and management principles.

Unit–IV:

Introductions to Information Availability: Business Continuity and Disaster Recovery Basics, Local business continuity techniques, Remote business continuity techniques, Disaster Recovery principles & techniques. Managing & Monitoring: Management philosophies (holistic vs. system & component), Industry management standards (SNMP, SMI-S, CIM), Standard framework applications, Key management metrics (thresholds, availability, capacity, security, performance), Metric analysis methodologies & trend analysis, Reactive and proactive management best practices, Provisioning & configuration change planning, Problem reporting, prioritization, and handling techniques, Management tools overview.

Unit–V:

Securing Storage and Storage Virtualization: Define storage security. List the critical security attributes for information systems, describe the elements of a shared storage model and security extensions, define storage security domains, List and analyze the common threats in each domain, identify different virtualization technologies, describe block-level and file level virtualization technologies and processes.

Course Outcomes: At the end of the course, the student should be able to

CO 1 : Understand the logical and physical components of a Storage infrastructure
CO 2 : Explore the various forms and types of Storage Virtualization
CO 3 : Discuss the storage architectures, including storage subsystems, DAS, SAN, NAS, and CAS
CO 4 : Describe the different roles in providing disaster recovery and business continuity capabilities
CO 5 : Distinguish different remote replication technologies

Textbooks:

1. Building Storage Networks, Marc Farley Osborne, Tata McGraw Hill, 2001.
2. Storage Networks: The Complete Reference, Robert Spalding and Robert Spalding, Tata McGraw Hill, 2003.
3. Meeta Gupta, Storage Area Network Fundamentals, Meeta Gupta, Pearson Education Ltd., 2002.

References:

1. Information Storage Retrieval Systems theory & Implementation, Gerald J Kowalski and Mark T Maybury, BS Publications, 2000.
2. Disaster Recovery & Business continuity, Thejendra BS, Shroff Publishers & Distributors, 2006.