Syllabus

VEER MADHO SINGH BHANDARI UTTARAKHAND TECHNICAL UNIVERSITY

(Formerly Uttarakhand Technical University, Dehradun Established by Uttarakhand State Govt. wide Act no. 415 of 2005)
Suddhowala, PO-Chandanwadi, Premnagar, Dehradun, Uttarakhand (Website- www.uktech.ac.in)

SYLLABUS

For

B.TECH

Cyber Security

2nd, 3rd and 4th Year

VEER MADHO SINGH BHANDARI UTTARAKHAND TECHNICAL UNIVERSITY

(Formerly Uttarakhand Technical University, Dehradun Established by Uttarakhand State Govt. wide Act no. 415 of 2005)
Suddhowala, PO-Chandanwadi, Premnagar, Dehradun, Uttarakhand (Website- www.uktech.ac.in)

SYLLABUS

For

B.TECH

Cyber Security

2ND Year

Effective From – Session 2023-24

Syllabus

SEMESTER-III													
S. NO.	Subject Codes	Category	Subject	Periods			Evaluation Scheme					Subject Total	Credit
							Sessional Exam			ESE			
				L	T	P	CT	TA	Total	TE	PE		
1	ECT-033	ESC	Digital Electronics	3	1	0	30	20	50	100		150	4
2	AHT-007	HSC	Technical Communication	2	1	0	30	20	50	100		150	3
3	CST-002	DC	Discrete Structure	3	1	0	30	20	50	100		150	4
4	CST-003	DC	Data Structures and Algorithms	3	1	0	30	20	50	100		150	4
5	CYT-101	DC	Unix/LINUX Security	3	1	0	30	20	50	100		150	4
6	CYT-102	DC	Introduction to Python Programming	3	1	0	30	20	50	100		150	4
7	CYT-103	DC	Cyber Security and Investigation Techniques	3	1	0	30	20	50	100		150	4
8	CSP-003	DLC	Data Structures and Algorithms Lab	0	0	2		25	25		25	50	1
9	CSP-005	DLC	Python Programming Lab	0	0	2		25	25		25	50	1
10	CYP-101	DLC	Internship-I/Mini Project-I*	0	0	2			50			50	1
11	GP-003	NC	General Proficiency						50			50	
			Total	20	7	6						1250	30
	*The Mini Project-I or Internship-I(3-4weeks) will be conducted during summer break after the II semester and will be assessed during the III semester												

Abbreviations: L-No. of Lecture hours per week, **T**-No. of Tutorial hours per week, **P**-No. of Practical hours per week, **CT**-Class Test Marks, **TA**-Marks of teacher's assessment including student's class performance and attendance, **PS**-Practical Sessional Marks, **ESE**-End Semester Examination, **TE**- Theory Examination Marks, PE- Practical External Examination Marks

1 Hr Lecture **1 Hr Tutorial** **2 or 3 Hr Practical**

1 Credit **1 Credit** **1 Credit**

Syllabus

SEMESTER-IV													
S. NO.	Subject Codes	Category	Subject	Periods			Evaluation Scheme					Subject Total	Credit
							Sessional Exam			ESE			
				L	T	P	CT	TA	Total	TE	PE		
1	CYT-104	DC	Cryptanalysis & Cyber Defense	3	1	0	30	20	50	100		150	4
2	AHT-006	HSC	Advance Applied Mathematics	3	1	0	30	20	50	100		150	4
3	CST-007	DC	Computer Organization and Architecture	3	1	0	30	20	50	100		150	4
4	CYT-105	DC	Software Engineering & Agile Practices	3	1	0	30	20	50	100		150	4
5	CST-009	DC	Formal Languages & Automata Theory	3	1	0	30	20	50	100		150	4
6	CST-011	DC	Database Management System	3	1	0	30	20	50	100		150	4
7	AHT-008	HSC	Universal Human Values	2	1	0	30	20	50	100		150	3
8	CSP-007	DLC	Computer Organization and Architecture Lab	0	0	2		25	25		25	50	1
9	CYP-102	DLC	Software Engineering & Agile Practices Lab	0	0	2		25	25		25	50	1
10	CSP-011	DLC	Database Management System Lab	0	0	2		25	25		25	50	1
11	GP-004	NC	General Proficiency						50				
			Total	17	7	6						1200	30
		DLC	Internship-II/Mini Project-II*	To be completed at the end of the fourth semester (during the Summer).									

Abbreviations: L-No. of Lecture hours per week, **T**-No. of Tutorial hours per week, **P**-No. of Practical hours per week, **CT**-Class Test Marks, **TA**-Marks of teacher's assessment including students class performance and attendance, **PS**-Practical Sessional Marks, **ESE**-End Semester Examination, **TE**- Theory Examination Marks, PE- Practical External Examination Marks

1 Hr Lecture **1 Hr Tutorial** **2 or 3 Hr Practical**

1 Credit **1 Credit** **1 Credit**

Syllabus

DIGITAL ELECTRONICS (ECT-033)

L:T:P:: 3:1:0 **Credits-04**

COURSE OBJECTIVES: The objectives of the course are to:

1. Understand the basics of digital electronics.
2. Understand the basics of Logic family.
3. Apply the knowledge of digital electronics to construct various digital circuits.
4. Analyze the characteristics and explain the outputs of digital circuits.
5. Evaluate and asses the application of the digital circuits.
6. Understand the design flow of VLSI Circuits

COURSEOUTCOMES: After completion of the course student will be able to:

1. Understand the Boolean algebra and minimization of digital functions.
2. Design and implement various combinational circuits.
3. Design and implement various sequential circuits.
4. Understand the digital logic families, semiconductor memories.
5. Design the digital circuits using VHDL

UNIT 1: **MINIMIZATION OF LOGIC FUNCTIONS**: Review of logic gate and Boolean algebra, DeMorgan's Theorem, SOP & POS forms, canonical forms, don't care conditions, K-maps up to 6 variables, Quine-McClusky's algorithm, X-OR & X-NOR simplification of K-maps, binary codes, code conversion.

UNIT 2: **COMBINATIONAL CIRCUITS**: Combinational circuit design, half and full adders, subtractors, serial and parallel adders, code converters, comparators, decoders, encoders, multiplexers, de-multiplexer, parity checker, driver &multiplexed display, BCD adder, Barrel shifter and ALU.

UNIT 3: **SEQUENTIAL CIRCUITS**: Building blocks like S-R, JK and master-slave JK FF, edge triggered FF, ripple and synchronous counters, shift registers, finite state machines, design of synchronous FSM, algorithmic state machines charts, designing synchronous circuits like pulse train generator, pseudo random binary sequence generator, clock generation

UNIT 4: **LOGIC FAMILIES & SEMICONDUCTOR MEMORIES**: TTL NAND gate, specifications, noise margin, propagation delay, fan-in, fan-out, tri-state TTL, ECL, CMOS families and their interfacing, memory elements, concept of programmable logic devices like FPGA, logic implementation using programmable devices.

UNIT 5: **VLSI DESIGN FLOW**: Design entry: schematic, FSM & HDL, different modelling styles in VHDL, data types and objects, dataflow, behavioral and structural modelling, synthesis and simulation VHDL constructs and codes for combinational and sequential circuits.

Syllabus

BOOKS:

1. Mano, Digital electronics,TMH,2007.
2. Malvino, Digital Principle and applications, TMH,2014.
3. Jain, Modern digital electronics, PHI, 2012.
4. Tocci, Digital Electronics, PHI,2001.
5. W.H.Gothmann, “Digital Electronics-An introduction to theory and practice”,PHI,2nd edition,2006

Syllabus

Technical Communication (AHT-007)

L:T:P:: 2:1:0 **Credits-03**

COURSE OBJECTIVES: The objectives of the course are:

1. Produce technical documents that use tools commonly employed by engineering and computer science professionals.
2. Communicate effectively in a professional context, using appropriate rhetorical approaches for technical documents, adhering to required templates, and complying with constraints on document format.
3. Clarify the nuances of phonetics, intonation and pronunciation skills.
4. Get familiarized with English vocabulary and language proficiency.

COURSE OUTCOMES: On successful completion of the course, the student will be able to:

1. Students will be enabled to **understand** the nature and objective of Technical Communication relevant for the work place as Engineers.
2. Students will **utilize** the technical writing for the purposes of Technical Communication and its exposure in various dimensions.
3. Students would imbibe inputs by presentation skills to **enhance** confidence in face of diverse audience.
4. Technical communication skills will **create** a vast know-how of the application of the learning to promote their technical competence.
5. It would enable them to **evaluate** their efficacy as fluent & efficient communicators by learning the voice-dynamics.

Unit -1 Fundamentals of Technical Communication:

Technical Communication: Introduction, Features; Distinction between General and Technical Communication; The flow of Communication: Downward; upward, Lateral or Horizontal; Barriers to Communication, Importance of communication

Unit - II Forms of Technical Communication:

Technical Report: Definition & importance; Thesis/Project writing: structure & importance; synopsis writing: Methods; Technical research Paper writing: Methods & style; Seminar & Conference paper writing; 7 Cs of effective business writing: concreteness, completeness, clarity, conciseness, courtesy, correctness, consideration.

Unit - III Technical Presentation: Strategies & Techniques

Syllabus

Presentation: Forms; interpersonal Communication; Class Room presentation; style;method, Public Speaking: method; Techniques: Clarity of substance; emotion; Humour; Modes of Presentation; Overcoming Stage Fear: Confident speaking; Audience Analysis & retention of audience interest; Methods of Presentation: Interpersonal; Impersonal; Audience Participation: Quizzes & Interjections

Unit - IV Technical Communication Skills

Interview skills; Group Discussion: Objective & Method; Seminar/Conferences Presentation skills: Focus; Content; Style; Argumentation skills: Devices: Analysis; Cohesion & Emphasis; Critical thinking; Nuances, exposition, narration and description

Unit - V Kinesics & Voice Dynamics:

Kinesics: Definitions; importance; Features of Body Language; Voice Modulation: Quality, Pitch; Rhythm; intonation, pronunciation, articulation, vowel and consonants sounds

Reference Books

1. Technical Communication – Principles and Practices by Meenakshi Raman & Sangeeta Sharma, Oxford Univ. Press, 2007, New Delhi.
2. Business Correspondence and Report Writing by Prof. R.C. Sharma & Krishna Mohan, Tata McGraw Hill & Co. Ltd., 2001, New Delhi.
3. Practical Communication: Process and Practice by L.U.B. Pandey; A.I.T.B.S. Publications India Ltd.; Krishan Nagar, 2014, Delhi.
4. Modern Technical Writing by Sherman, Theodore A (et.al); Apprentice Hall; New Jersey; U.S.
5. A Text Book of Scientific and Technical Writing by S.D. Sharma; Vikas Publication, Delhi.
6. Skills for Effective Business Communication by Michael Murphy, Harward University, U.S. Business Communication for Managers by Payal Mehra, Pearson Publication, Delhi.

Syllabus

DISCRETE STRUCTURE (CST-002)

L:T:P:: 3:1:0 **Credits-04**

COURSE OBJECTIVES: The objectives of the course are to:

1. To introduce several Discrete Mathematical Structures to serve as tools in the development of theoretical computer science.
2. Transform a given problem into a combination of several simpler statements, reach at a solution and prove it logically.
3. Enhance the ability to reasoning and presenting the mathematically accurate argument.
4. Apply the abstract concepts of graph theory in the modelling and solving of non-trivial.

COURSE OUTCOMES: On successful completion of the course, the student will be able to:

1. Develop new models to represent and interpret the data.
2. Apply knowledge of mathematics, probability & statistics, graph theory and logics.
3. Interpret statements presented in disjunctive normal form and determine their validity by applying the rules and methods of propositional calculus.
4. Reformulate statements from common language to formal logic using the rules of propositional and predicate calculus.
5. Apply graph theory in solving computing problems.

Unit 1- Set Theory: Introduction to set theory, set operations, Algebra of Sets, Combination of sets, Duality, Finite and infinite sets, Classes of sets, Power sets, Multi sets, Cartesian Product, Representation of relations, Types of relation, Binary relation, Equivalence relations and partitions, Mathematics Induction.

Function and its types: Composition of function and relations, Cardinality and inverse relations, Functions, logic and proofs injective, surjective and bijective functions.

Unit 2- Propositional Calculus: Basic operations; AND(^), OR(v), NOT(~), True value of a compound statement, propositions, tautologies, and contradictions. Partial ordering relations and lattices.

Lattice theory: Partial ordering, posets, lattices as posets, properties of lattices as algebraic systems, sublattices, and some special lattices.

Unit 3-Combinations: The Basic of Counting**,** Pigeonhole Principles, Permutations and Combinations, Principle of Inclusion and Exclusion.

Recursion and Recurrence Relation: linear recurrence relation with constant coefficients, Homogeneous solutions, Particular solutions, and Total solution of a recurrence relation using generating functions.

Syllabus

Unit 4- Algebraic Structures: Definition, elementary properties of Algebraic structures, examples of a Monoid, sunmonoid, semigroup, groups and rings, Homomorphism, Isomorphism and automorphism, Subgroups and Normal subgroups, Cyclic groups, Integral domain and fields, Rings, Division Ring.

Unit 5- Graphs and Trees: Introduction to graphs, Directed and undirected graphs, Homomorphic and Isomorphic graphs, Subgraphs, cut points and bridges, Multigraph and Weighted graphs, Paths and circuits, Shortest path in a weighted graph, Eulerian path and circuits, Hamilton paths and circuits, Planar graphs, Euler's formula, Trees, Rooted trees, Spanning trees and cut-sets, Binary trees and its traversals.

TEXTBOOKS:

1. Discrete and combinatorial mathematics-An applied introduction-5th edition- Ralph P. Grimaldi, Pearson Education.
2. Discrete Mathematics for Computer Scientists & Mathematicians, J.L. Mott. A. Kandel, T.P. Baker, Prentice Hall.

REFERENCE BOOKS:

1. Discrete mathematical with graph theory, edgar G. Goodaire, 3rd Edition, Pearson Education.
2. Discrete Mathematics and its Applications, Kenneth H. Rosen, Fifth Edition. TMH.
3. Mathematical foundations of computer science-Dr S. Chandra sekharaiah-Prism books Prv. Lt.
4. Discrete mathematical structures Theory and applications-malik & Sen.
5. Logic and Discrete Mathematics, Grass Mann & Trembley, Person Education.
6. Discrete mathematical structures with applications to Comp. Science- J. P. Tremblay and R. Manohar, Tata-McGraw-Hill publications.
7. Elements of DISCRETE MATHEMATICS – A computer-oriented Approach – C L Liu, D P Mohapatra. Third Edition, Tata McGraw Hill

Syllabus

DATA STRUCTURES AND ALGORITHMS (CST-003)

L:T:P:: 3:1:0 **Credits-04**

Course Objectives: The objectives of this course are to:

1. Introduce the fundamentals of Data Structures, Abstract concepts and how these concepts are useful in problem-solving.
2. Analyze step by step and develop algorithms to solve real-world problems.
3. Implement various data structures, viz. Stacks, Queues, Linked Lists, Trees and Graphs.
4. Understand various searching & sorting techniques

Course Outcomes: On successful completion of the course, the student will be able to:

1. Compare functions using asymptotic analysis and describe the relative merits of worst-case, average-case, and best-case analysis.
2. Become familiar with a variety of sorting algorithms and their performance characteristics (e.g., running time, stability, space usage) and be able to choose the best one under a variety of requirements.
3. Understand and identify the performance characteristics of fundamental algorithms and data structures and be able to trace their operations for problems such as sorting, searching, selection, operations on numbers, and graphs.
4. Solve real-world problems using arrays, stacks, queues, and linked lists.
5. Become familiar with the major graph algorithms and their analyses. Employ graphs to model engineering problems when appropriate.

Unit 1-Introduction: Basic Terminologies: Elementary Data Organizations, Data Structure Operations: insertion, deletion, traversal etc.; Analysis of an Algorithm, Asymptotic Notations, Time-Space trade-off.

Searching: Linear Search and Binary Search Techniques and their complexity analysis.

Unit 2-Stacks and Queues: ADT Stack and its operations: Algorithms and their complexity analysis, Applications of Stacks: Expression Conversion and evaluation – corresponding algorithms and complexity analysis. ADT queue, Types of Queues: Simple Queue, Circular Queue, Priority Queue; Operations on each type of Queues: Algorithms and their analysis.

Unit 3-Linked Lists: Singly linked lists: Representation in memory, Algorithms of several operations: Traversing, Searching, Insertion into, Deletion from the linked list; Linked representation of Stack and Queue, Header nodes, Doubly linked list: operations on it and algorithmic analysis; Circular Linked Lists: all operations their algorithms and complexity analysis.

Syllabus

Unit 4-Trees and Graphs: Basic Tree Terminologies, Different types of Trees: Binary Tree, Threaded Binary Tree, Binary Search Tree, AVL Tree; Tree operations on each of the trees and their algorithms with complexity analysis. Applications of Binary Trees. B Tree, B+ Tree: definitions, algorithms and analysis.

Graphs: Basic Terminologies and Representations, Graph search and traversal algorithms and complexity analysis.

Unit 5-Sorting and Hashing: Objective and properties of different sorting algorithms: Selection Sort, Bubble Sort, Insertion Sort, Quick Sort, Merge Sort, Heap Sort; Performance and Comparison among all the methods,

Hashing: Symbol table, Hashing Functions, Collision-Resolution Techniques

TEXTBOOKS:

1. An Introduction to Data Structures with Applications. by Jean-Paul Tremblay & Paul G. Sorenson Publisher-Tata McGraw Hill.
2. Ritika Mehra, Data Structures Using C, Pearson Education.
3. Data Structures using C & C++ -By Ten Baum Publisher – Prentice-Hall International**.**

REFERENCE BOOKS:

1. Schaum's Outlines Data structure Seymour Lipschutz Tata McGraw Hill 2nd Edition.
2. Fundamentals of Computer Algorithms by Horowitz, Sahni, Galgotia Pub. 2001 ed.
3. Fundamentals of Data Structures in C++-By Sartaj Sahani.
4. Data Structures: A Pseudo-code approach with C -By Gilberg&Forouzan Publisher-Thomson Learning.

Syllabus

UNIX /LINUX SECURITY (CYT-101)

L:T:P:: 3:1:0 **Credits-04**

Course Objective:

1. To provide an introduction to an operating system that is assembled under the model of free and open source software development and distribution.
2. To develop software in and for Linux/UNIX environments.
3. Understanding the basic set of commands and utilities in Linux/UNIX systems.
4. To learn to develop software for Linux/UNIX systems.
5. To understand the inner workings of UNIX-like operating systems.

Course Outcomes:

Upon completing the course, students will be able to:

1. Learn the basics of Unix operating syatem
2. Plan, Deploy and Linux Server
3. Monitor and Manage Linux Server.
4. Perform the tasks of a Network Administrator.
5. Write programme in using shell programming.

Prerequisites: Basics of DOS.

COURSE OF CONTENTS

UNIT I

Evolution of Unix OS, philosophy. Features of Unix operating system, Basic Architecture of Unix/Linux system, features of Kernel and Shell. Unix File system - Boot block, super block,Inode table, data blocks, How Unix/Linux kernel access files, Unix/Linux standard file system.

UNIT II

Basic UNIX environment: Basic commands, directory management, pipes, tee, I/Oredirection and other utilities. Advanced commands: File system and process management commands, Shell, Pattern matching, Navigating the File Systems.

UNIT III

Unix editor: VI editor, Creating new files. Text addition, deletion and changes. Dealing With sentences and paragraphs. Searching. Cut, paste and copy. Running C/C++ programs.Shell programming: Features of shell. Shell variables. Control statements. Advance shell programming: Command line arguments. Interactive shell scripts. Debugging of shell scripts. Communication facilities in Unix, Mathematical commands.

Syllabus

UNIT IV

Structure of Unix operating system: Structure of Unix kernel, Unix system calls.Unix system: File system calls, Process management calls.Advance Filter: Awk: Number processing, Interface with shell, functions.

UNIT V

Unix system administration: Adding and removing users. User accounting. Adding andremoving hardware. Performing backups and restore. Disk space management.Unix system administration: Configuring the kernel. Network management in Unix.Performance analysis. Unix Desktop. Installation of Unix/Linux system – Unix/Linux Installion requirement, complete Procedure steps, Partitioning the Hard drive, System startup and shut-down process, init and run levels. File system mounting, lpstat, backup strategy, installing software on Unix/Linux.

BOOKS RECOMMENDED:

[1] Sumitabh Das, UNIX Operating Systems,Tata McGraw Hills publication, 2006.

[2] Syed MansoorSarwar, Robert Kortskey,UNIX,Pearson Education, 2004.

[3] Sumitabha Das,Unix concepts and Application,TataMcGraw Hill, 2008.

[4] David Bandel and R. Napier, Using Linux,6th Ed., Pearson Education, 2014

Syllabus

Introduction to Python Programming (CYT-102)

L:T:P:: 3:1:0 **Credits-04**

Course objectives

1. Learn the syntax and semantics of the Python programming language.
2. Illustrate the process of structuring the data using lists, tuples
3. Appraise the need for working with various documents like Excel, PDF, Word and Others.
4. Demonstrate the use of built-in functions to navigate the file system.
5. Implement the Object Oriented Programming concepts in Python.

Course outcome

At the end of the course the student will be able to:

1. Learn the of Python programming language
2. Demonstrate proficiency in handling loops and creation of functions.
3. Identify the methods to create and manipulate lists, tuples and dictionaries.
4. Develop programs for string processing and file organization
5. Interpret the concepts of Object-Oriented Programming as used in Python.

UNIT-1

Python Basics: Entering Expressions into the Interactive Shell, The Integer, Floating-Point, and String Data Types, String Concatenation and Replication, Storing Values in Variables, Your First Program, Dissecting Your Program, Flow control: Boolean Values, Comparison Operators, Boolean Operators,Mixing Boolean and Comparison Operators, Elements of Flow Control, Program Execution, Flow Control Statements, Importing Modules,Ending a Program Early with sys.exit(), Functions: def Statements with Parameters, Return Values and return Statements,The None Value, Keyword Arguments and print(), Local and Global Scope, The global Statement, Exception Handling, A Short Program: Guess the Number

UNIT-2

Lists: The List Data Type, Working with Lists, Augmented Assignment Operators, Methods, Example Program: Magic 8 Ball with a List, List-like Types: Strings and Tuples, References, Dictionaries and Structuring Data: The Dictionary Data Type, Pretty Printing, Using Data Structures to Model Real-World Things,

Syllabus

UNIT-3

Manipulating Strings: Working with Strings, Useful String Methods, Project: Password Locker, Project: Adding Bullets to Wiki Markup Reading and Writing Files: Files and File Paths, The os.path Module, The File Reading/Writing Process, Saving Variables with the shelve Module,Saving Variables with the print.format() Function, Project: Generating Random Quiz Files, Project: Multiclipboard,

UNIT-4

Organizing Files: The shutil Module, Walking a Directory Tree, Compressing Files with the zipfile Module, Project: Renaming Files with American-Style Dates to European-Style Dates,Project: Backing Up a Folder into a ZIP File, Debugging: Raising Exceptions, Getting the Traceback as a String, Assertions, Logging, IDLE‟s Debugger.

UNIT-5

Classes and objects: Programmer-defined types, Attributes, Rectangles, Instances as return values, Objects are mutable, Copying, Classes and functions: Time, Pure functions, Modifiers, Prototyping versus planning, Classes and methods: Object-oriented features, Printing objects, Another example, A more complicated example,Theinit method, The __str__ method, Operator overloading, Type-based dispatch, Polymorphism, Interface and implementation.

Text Books

1. Al Sweigart,“Automate the Boring Stuff with Python”,1 stEdition, No Starch Press, 2015.
2. Allen B. Downey, “Think Python: How to Think Like a Computer Scientist”, 2 nd Edition, Green Tea Press, 2015.

Syllabus

CYBER SECURITY AND INVESTIGATION TECHNIQUES (CYT-103)

L:T:P:: 3:1:0 **Credits-04**

COURSE OBJECTIVE:

1. Understand the real world security challenges.
2. Understand the basic internet security.
3. To protect the remote access and local computing devices.
4. To apply the tools and utilities for Network threats & Attacks.

COURSE OUTCOME:

1 Understanding the basics of Cyber Security access and monitoring systems.

2 Understanding the concepts of intrusion detection and security challenges.

3 Implementing the protection tools for local and intrusion detection.

4 Applying the network protection systems.

5 Appreciate the vulnerabilities, identifying and defending against threats.

Contents		Hours
Unit 1	Introduction to Cyber Security: Overview of Cyber Security, Internet Governance – Challenges and Constraints, Cyber Threats:- Cyber Warfare-Cyber Crime-Cyber terrorism-Cyber Espionage, Need for a Comprehensive Cyber Security Policy, Need for a Nodal Authority, Need for an International convention on Cyberspace.	8
Unit 2	Cyber Security Vulnerabilities and Cyber Security Safeguards: Poor Cyber Security Awareness. Cyber Security Safeguards- Overview, Access control, Audit, Authentication, Biometrics, Cryptography, Deception, Denial of Service Filters, Ethical Hacking, Firewalls, Intrusion Detection Systems, Response,Scanning, Security policy, Threat Management.	8
Unit 3	Securing Web Application, Services and Servers: Introduction, Basic security for HTTP Applications and Services, Basic Security for SOAP Services, Identity Management and Web Services, Authorization Patterns, Security Considerations, Challenges.	8
Unit 4	Intrusion Detection and Prevention: Intrusion, Physical Theft, Abuse of Privileges, Unauthorized Access by Outsider, Malware infection, Intrusion detection and Prevention Techniques, Anti-Malware software, Network based Intrusion detection Systems, Network based Intrusion Prevention Systems, Hostbased Intrusion prevention Systems,	8

Syllabus

Unit 5	Prevention Systems: Network based Intrusion Prevention Systems, Host based Intrusion prevention Systems, Security Information Management, Network Session Analysis, System Integrity Validation. Security Information Management, Network Session Analysis, System Integrity Validation.	8

Text Books

1. Cyber security Essentials, Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short, Sybex, October 2018

Reference Books

1. Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, B.B.Gupta, D.P.Agrawal, Haoxiang Wang, CRC Press, 2018

2. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press

Syllabus

DATA STRUCTURES AND ALGORITHMS LAB (CSP-003)

L:T:P:: 0:0:2 **Credits-01**

Course Objectives: The objectives of this course are to:

1. Analyse step by step development of algorithms to solve real-world problems.
2. Implement various data structures, viz. Stacks, Queues, Linked Lists, Trees and Graphs.
3. Understand various data searching & sorting techniques.

Course Outcomes: On successful completion of the course, the student will be able to:

1. Develop programs using dynamic memory allocation and linked list ADT.
2. Apply Stack and Queue to solve problems.
3. Implement the concept of hashing in real-time dictionaries.
4. Identify and implement suitable data structures for the given problem.
5. Solve real-world problems by finding the minimum spanning tree and the shortest path algorithm.

LIST OF EXPERIMENTS:

1. Write programs to implement the following using an array.
   a) Stack ADT
   b) Queue ADT
2. Write programs to implement the following using a singly linked list.
   a) Stack ADT
   b) Queue ADT
3. Write a program to implement the deque (double-ended queue) ADT using a doubly linked list.
4. Write a program to perform the following operations:
   a) Insert an element into a binary search tree.
   b) Delete an element from a binary search tree.
   c) Search for a key element in a binary search tree.
5. Write a program to implement circular queue ADT using an array.
6. Write a program to implement all the functions of a dictionary (ADT) using hashing.
7. Write a program to perform the following operations on B-Trees and AVL-trees:
   a) Insertion.
   b) Deletion.
8. Write programs for implementing BFS and DFS for a given graph.
9. Write programs to implement the following to generate a minimum cost-spanning tree:

a) Prim's algorithm.

b) Kruskal's algorithm.

10. Write a program to solve the single source shortest path problem.

(Note: Use Dijkstra's algorithm).

11. Write a program that uses non-recursive functions to traverse a binary tree in:

a) Pre-order.

b) In-order.

c) Post-order.

12. Write programs for sorting a given list of elements in ascending order using the following sorting methods:

a) Quick sort.

b) Merge sort.

Syllabus

PYTHON PROGRAMMING LAB (CSP-005)

L:T:P:: 0:0:2 **Credits-01**

COURSE OBJECTIVES: The objectives of this course are to:

1. Learn and understand Python programming basics and control statements.
2. Illustrate the applications of string handling and regular expressions in building Python programs using functions.
3. Discover the use of supported data structures like lists, dictionaries, and tuples in Python.
4. Understand a range of Object-Oriented Programming and in-depth data and information processing techniques.
5. Apply the concepts of file I/O in python.

COURSE OUTCOMES: On successful completion of the course, the student will be able to:

1. Demonstrate the basic concepts of python programming with the help of data types, operators and expressions, and console input/output.
2. Apply the concept of Control Structures in Python to solve any given problem.
3. Demonstrate operations on built-in container data types (list, tuple, set, dictionary) and strings.
4. Ability to explore python, especially the object-oriented concepts and the built-in objects of Python.
5. Implement the concepts of file handling using packages.

LIST OF PROGRAMS:

Exercise 1 - Basics

a) Running instructions in Interactive interpreter and a Python Script

b) Write a program to purposefully raise Indentation Error and Correct it

Exercise 2 - Operations

a) Write a program to compute distance between two points taking input from the user (Pythagorean Theorem)

b) Write a program add.py that takes 2 numbers as command line arguments and prints its sum.

Exercise - 3 Control Flow

a) Write a Program for checking whether the given number is a even number or not.

b) Using a for loop, write a program that prints out the decimal equivalents of 1/2, 1/3, 1/4, . . . ,1/10

c) Write a program using a for loop that loops over a sequence.

d) Write a program using a while loop that asks the user for a number, and prints a countdown from that number to zero.

Exercise 4 - Control Flow - Continued

a) Find the sum of all the primes below two million. Adding the previous two terms, each new term in the Fibonacci sequence

is generated. By starting with 1 and 2, the first 10 terms will be:

1, 2, 3, 5, 8, 13, 21, 34, 55, 89, ...

b) By considering the terms in the Fibonacci sequence whose values do not exceed four million,find the sum of the even-valued terms.

c) Linear search and Binary search

d) Selection sort, Insertion sort

Exercise - 5 - DS

a) Write a program to count the numbers of characters in the string and store them in a dictionary data structure

b) Write a program to use split and join methods in the string and trace a birthday with a dictionary data structure.

Exercise - 6 DS - Continued

a) Write a program combine_lists that combines these lists into a dictionary.

b) Write a program to count frequency of characters in a given file. Can you use character frequency to tell whether the given file is a Python program file, C program file or a text file?

Exercise - 7 Files

a) Write a program to print each line of a file in reverse order.

b) Write a program to compute the number of characters, words and lines in a file.

Exercise - 8 Functions

a) Write a function ball_collide that takes two balls as parameters and computes if they are colliding. Your function should return a Boolean representing whether or not the balls are colliding.

Hint: Represent a ball on a plane as a tuple of (x, y, r), r being the radiusIf (distance between two balls centers) <= (sum of their radii), then (they are colliding)

b) Find the mean, median, and mode for the given set of numbers in a list.

Exercise - 9 Functions - Continued

a) Write a function nearly_equal to test whether two strings are nearly equal. Two strings a and bare nearly equal when a single mutation on b can generate a.

b) Write a function dups to find all duplicates in the list.

c) Write a function unique to find all the unique elements of a list.

Exercise - 10 - Functions –Problem-Solving

a) Write a function cumulative_product to compute the cumulative product of a list of numbers.

b) Write a function reverse to reverse a list. Without using the reverse function.

c) Write a function to compute gcd, lcm of two numbers. Each function shouldn’t exceed one line.

Exercise - 11–Python Packages

a) Install packages requests, flask and explore them. using (pip)

b) Plot graphs using python and Matplotlib.

c) Data Analysis using numpy and Pandas Libraries

Syllabus

INTERNSHIP-I/MINI PROJECT-I(CYP-101)

L:T:P:: 0:0:2 **Credits-01**

ABOUT INTERNSHIP/ MINI PROJECT

It is an organized method or activity of enhancing and improving engineering students' skill sets and knowledge, which boosts their performance and consequently helps them meet their career objectives. Industrial Training is essential in developing the practical and professional skills required for an Engineer and an aid to prospective employment.

OBJECTIVES OF INTERNSHIP/ MINI PROJECT: The objectives of this course is to:

1. Expose the students to the actual working environment and enhance their knowledge and skill from what they have learned in college.
2. Enhance the good qualities of integrity, responsibility, and self-confidence. Students must follow all ethical values and good working practices.
3. Help the students with the safety practices and regulations inside the industry and to instils the spirit of teamwork and good relationship between students and employees.

COURSE OUTCOMES: On successful completion of the course, the student will be able to:

1. Understand organizational issues and their impact on the organization and employees.
2. Identify industrial problems and suggest possible solutions.
3. Relate, apply and adapt relevant knowledge, concepts and theories within an industrial organization, practice and ethics.
4. Apply technical knowledge in an industry to solve real world problems.
5. Demonstrate effective group communication, presentation, self-management, and report writing skills**.**

Syllabus

CRYPTO-ANALYSIS AND CYBER DEFENSE(CYT-104)

L:T:P:: 3:1:0 **Credits-04**

COURSE OBJECTIVES

1.To understand the mathematics behind Cryptography.

2.To understand the security concerns and vulnerabilities

3. To familiarize with different types of cryptosystems

4. To create an awareness for the design of various cryptographic primitives

5.To analyze different types of attacks on various cryptosystems.

COURSE OUTCOMES :At the end of the course the students should be able to:

1.To learn the importance of number theory in designing crypto systems;

2.To design public and private key cryptosystems;

3.To do cryptanalysis of various cryptosystems.

4. To implement cryptographic algorithms

5. To structure Privacy issues and able to resolve them

Contents		Hours
Unit 1	Introduction to Security: Security Concepts, Security Attacks, Antivirus bypassing, Password Attacks and Web browser exploitation, Security Services and Mechanisms, A Security Model, Classical Encryption Techniques: Symmetric Cipher Model, Substitution techniques, Transposition Techniques.	8
Unit 2	Block Ciphers and DES: Traditional Block Cipher Structure, DES, DES Example, Strength of DES, Differential and Linear Cryptanalysis, Block Cipher Design Principles. AES: Finite Field Arithmetic, AES Structure	10
Unit 3	AES Transformation Functions, AES Example, AES Implementation. Block Cipher Operation: Multiple Encryption and Triple DES, Modes of Operation, Pseudorandom Number Generation and Stream Ciphers: Principles and Pseudorandom Number Generation,	8
Unit 4	Pseudorandom Number, Generators, Pseudorandom Number Generation using a Block Cipher, Stream, Ciphers, RC4.Public-key Cryptography and RSA: Principles of Public-Key Cryptosystems, the RSA algorithm.	10

Syllabus

Unit 5	Other Public-key Cryptosystems: Diffie-Hellman Key Exchange, ElGamal Cryptosystem, Investigating Information-hiding: Investigating Information-hiding, Scrutinizing E-mail, Validating E-mail header information, Tracing Internet access, Tracing memory in real-time.	9

Text Books:

1. Behrouz A. Forouzan and Debdeep Mukhopadhyay, Cryptography & Network Security, Second Edition, Tata McGraw Hill, New Delhi, 2010

2. Douglas R. Stinson, "Cryptography: Theory and Practice", Third Edition, CRC Press.

3. William Stallings, "Cryptography and Network Security – Principles and Practices", Pearson Education, Fourth Edition, 2006.

Reference Books:

1. Atul Kahate, "Cryptography and Network Security", 2nd Edition, Tata McGraw Hill, 2003.

2. Bernard Menezes, Network Security and Cryptography-Cengage Learning India, 2011

3. Bruce Schneier, "Applied Cryptography: Protocols, Algorthms, and Source Code in C", Second Edition, John Wiley and Sons Inc, 2001.

4. Thomas Mowbray, "Cybersecurity : Managing Systems Conducting Testing, and Investigating Intrusions", John Wiley, 2013

5. Wenbo Mao, " Modern Cryptography- Theory & Practice", Pearson Education, 2006.

Syllabus

Advanced Applied Mathematics (AHT-006)

L:T:P:: 3:1:0 **Credits-4**

COURSE OBJECTIVES: The objectives of the course are to:

1. The idea of Laplace transform of functions and their applications.
2. The idea of Fourier transform of functions and their applications.
3. Evaluate roots of algebraic and transcendental equations.
4. Interpolation, numerical differentiation& integration and the solution of differential equations.
5. Acquaintance with statistical analysis and techniques.

COURSE OUTCOMES:

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

1. Remember the concept of Laplace transform and apply in solving real life problems.
2. Apply the concept of Fourier transform to evaluate engineering problems.
3. Understand to evaluate roots of algebraic and transcendental equations.
4. Solve the problem related interpolation, differentiation, integration and the solution of differential equations.
5. Understand the concept of correlation, regression, moments, skewness and kurtosis and curve fitting.

Module 1: Laplace Transform: **(8 hours)**

Definition of Laplace transform, Existence theorem, Laplace transforms of derivatives and integrals, Initial and final value theorems, Unit step function, Dirac- delta function, Laplace transform of periodic function, Inverse Laplace transform, Convolution theorem, Application to solve linear differential equations.

Module 2: Fourier Transforms: **(8 hours)**

Fourier integral, Fourier sine and cosine integral, Complex form of Fourier integral, Fourier transform,Inverse Fourier transforms, Convolution theorem, Fourier sine and cosine transform, Applications of Fourier transform to simple one dimensional heat transfer equations.

Module 3: Solution of Algebraic & Transcendental equations and Interpolation: **(8 hours)**

Number and their accuracy, Solution of algebraic and transcendental equations: Bisection method, Iteration method, Newton-Raphson method and Regula-Falsi method. Rate of convergence of these methods (without proof), Interpolation: Finite differences, Relation between operators, Interpolation using Newton's forward and backward difference formula, Interpolation with unequal intervals: Newton's divided difference and Lagrange's formula.

Module 4: Numerical differentiation & Integration and Solution of ODE: **(8 hours)**

Numerical Differentiation, Numerical integration: Trapezoidal rule, Simpson's 1/3rd and 3/8 rule,Runge-Kutta method of fourth order for solving first order linear differential equations, Milne's predicator-corrector method.

Module 5: Statistical Techniques: (8 hours)

Introduction: Measures of central tendency, Moments, Skewness, Kurtosis, Curve fitting: Method of least squares, Fitting of straight lines, Fitting of second degree parabola, Exponential curves. Correlation and rank correlation, Regression analysis: Regression lines of y on x and x on y, Regression coefficients, Properties of regressions coefficients and non-linear regression.

Reference Books:

1. E. Kreyszig: Advanced Engineering Mathematics, John Wiley & Sons,10th ed.
2. B.V. Ramana: Higher Engineering Mathematics,McGrawHill.
3. Peter V.O'Neil: Advanced Engineering Mathematics, Cengage Learning,7th ed.
4. B.S. Grewal: Higher Engineering Mathematics, Khanna Publishers, 44th ed.
5. T.Veerarajan: Engineering Mathematics (for semester III), McGrawHill, 3rd ed.
6. R.K. Jain and S.R.K. Iyenger: Advance Engineering Mathematics,Narosa PublishingHouse,Std. ed.
7. P. Kandasamy, K. Thilagavathy, K. Gunavathi: Numerical Methods, S. Chand.
8. S.S. Sastry: Introductory methods of numerical analysis, Prentice Hall India, 5thed.
9. N.P. Bali and Manish Goyal: Computer Based Numerical and Statistical Techniques,Laxmi Publications, 5th ed.
10. J.N. Kapur: Mathematical Statistics, S. Chand &Company.
11. D.N.Elhance,V. Elhance&B.M. Aggarwal: Fundamentals of Statistics,Kitab Mahal.

Syllabus

COMPUTER ORGANIZATION AND ARCHITECTURE (CST-007)

L:T:P:: 3:1:0 **Credits-04**

COURSE OBJECTIVES: The objectives of this course are to:

1. Thoroughly understand the basic structure and operation of a digital computer.
2. Study the different communication methods with I/O devices and standard I/O interfaces.
3. Learn the various instruction modes, Addressing modes and RISC and CISC Architecture
4. Study the various memory architecture.

COURSE OUTCOMES: On successful completion of the course, the student will be able to:

1. Draw the functional block diagram of a single bus architecture of a computer and describe the function of the instruction execution cycle, RTL interpretation of instructions.
2. Given a CPU organization and instruction, design a memory module and analyze its operation by interfacing with the CPU.
3. Design the connection between I/O address from the CPU and the I/O interface.
4. Understand the concept of Pipelining and multiprocessor.
5. Draw a flowchart for concurrent access to memory and cache coherency in parallel processors.

Unit 1- Functional Blocks of a Computer: CPU, Memory, Input-Output Subsystems, Control Unit. Instruction Set Architecture of a CPU – Registers, Instruction Execution Cycle, RTL Representation and Interpretation of Instructions, Addressing Modes, Instruction Set. Case Study – Instruction Sets of Some Common CPUs, RISC and CISC Architecture.

Unit 2- Basic Processing Unit: Signed Number Representation, Fixed Point Arithmetic, Addition and Subtraction of Signed Numbers, Multiplication of Positive Numbers, Signed Operand Multiplication Algorithm, Booth Multiplication Algorithm, division algorithm, floating point numbers and its arithmetic operation. Fundamental Concepts: Execution of a Complete Instruction, Multiple Bus Organization, Hardwired Control, Micro Programmed Control.

Unit 3- Peripheral Devices and their Characteristics: Input-Output Subsystems, I/O Device Interface, I/O Transfers– Program Controlled, Interrupt Driven and DMA, Software Interrupts and Exceptions, Programs and Processes – Role of Interrupts in Process State Transitions, I/O Device Interfaces – SCII, USB.

Unit 4- Pipelining& Multiprocessor: Basic Concepts of Pipelining, Throughput and Speedup, Instruction Pipeline, Pipeline Hazards, Introduction to Parallel Processors, Symmetric Shared Memory and Distributed Shared Memory Multiprocessors, Performance Issues of Symmetric and Distributed Shared Memory, Synchronization.

Syllabus

Unit 5- Memory Organization: Basic Concepts, Concept of Hierarchical Memory Organization, Main Memory: RAM, ROM, Speed, Size and cost, Cache Memory and its Mapping, Replacement Algorithms, Write Policies, Virtual Memory, Memory Management Requirements, Associative Memory, Secondary storage devices.

TEXTBOOKS:

1. William Stallings, Computer Organization and architecture, 11th edition (2022), Pearson Education.
2. David A. Patterson and John L. Hennessy "Computer Organization and Design: The Hardware/Software Interface" , 5th Edition, Elsevier.
3. M. Morris Mano, "Computer System Architecture", Third Edition, Pearson Education.

REFERENCE BOOKS:

1. Microprocessor Architecture, Programming, and Applications with the 8085 -Ramesh S. Gaonkar Pub: Penram International.
2. CarlHamacher" Computer Organization and EmbeddedSystems", 6th Edition, McGraw Hill HigherEducation.
3. Miles Murdoccaa and Vincent Heuring"Computer Architecture and Organization: An integrated Approach" 2nd edition,Wiley Publication.

Syllabus

SOFTWARE ENGINEERING & AGILE PRACTICE (CYT-105)

L:T:P:: 3:1:0 **Credits-04**

Course Objectives:

1. Understand the principles, methodologies, and best practices of software engineering.
2. Explore the Agile Manifesto and its applications in modern software development.
3. Learn to design, implement, and maintain software systems using industry-standard tools and techniques.
4. Develop skills in collaborative teamwork, communication, and problem-solving within Agile development environments.
5. Gain practical experience in applying Agile methodologies to real-world software projects.

Course Outcomes:

1. Demonstrate proficiency in software development lifecycle models, including Agile methodologies like Scrum and Kanban.
2. Apply software engineering principles to analyze, design, implement, and test software solutions.
3. Employ Agile practices such as iteration planning, backlog grooming, and continuous integration to manage project development effectively.
4. Collaborate effectively within Agile teams, utilizing communication tools and techniques to facilitate project progress and resolve conflicts.
5. Evaluate the effectiveness of Agile practices in improving software quality, productivity, and customer satisfaction.

Unit 1: Introduction to Software Engineering

Overview of Software Engineering, Software Development Life Cycle (SDLC), Importance of Software Engineering in modern development practices Software Engineering principles and methodologies Challenges in Software Engineering

Unit 2: Agile Principles and Values

Introduction to Agile Manifesto, Principles of Agile Software Development, Agile methodologies: Scrum, Kanban, XP, Lean, etc., Comparison of Agile methodologies, Agile roles and responsibilities

Unit 3: Scrum Framework

Introduction to Scrum, Scrum roles: Scrum Master, Product Owner, Development Team,Scrum artifacts: Product Backlog, Sprint Backlog, Increment, Scrum events: Sprint Planning, Daily Scrum,,Sprint Review, Sprint Retrospective Sprint execution and monitoring

Unit 4: Agile Engineering Practices

Test-Driven Development (TDD), Continuous Integration (CI) and Continuous Delivery (CD), Pair Programming, Refactoring and Code Smells, Agile architecture and design principles

Syllabus

Unit 5: Advanced Agile Topics

Scaling Agile: SAFe, LeSS, Nexus, etc., Agile Metrics and Reporting, Agile in distributed teams, Agile transformation and organizational change, Agile maturity models

References:

- "Agile Estimating and Planning" by Mike Cohn
- "Scrum: The Art of Doing Twice the Work in Half the Time" by Jeff Sutherland
- "Lean Software Development: An Agile Toolkit" by Mary Poppendieck and Tom Poppendieck
- "Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation" by Jez Humble and David Farley

Syllabus

FORMAL LANGUAGES & AUTOMATA THEORY (CST-009)

L:T:P:: 3:1:0 **Credits-04**

COURSE OBJECTIVES: The objectives of this course are to:

1. Introduce the student to the concepts of theory of computation in computer science.
2. Acquire insights into the relationship among formal languages, formal grammars, and automata.
3. Learn to design automats and Turing machine.

COURSE OUTCOMES: On successful completion of the course, the student will be able to:

1. Apply the knowledge of automata theory, grammars & regular expressions for solving the problem.
2. Analyze the give automata, regular expression & grammar to know the language it represents.
3. Design Automata & Grammar for pattern recognition and syntax checking.
4. Distinguish between decidability and un-decidability of problems.
5. Identify limitations of some computational models and possible methods of proving them.

Unit 1- Introduction: Alphabets, Strings and Languages; Automata and Grammars, Deterministic finite Automata (DFA)-Formal Definition, Simplified notation: State transition graph, Transition table, Language of DFA, Nondeterministic finite Automata (NFA), NFA with epsilon transition, Language of NFA, Equivalence of NFA and DFA, Minimization of Finite Automata, Distinguishing one string from other, Myhill-Nerode Theorem

Unit 2- Regular Expressions: Definition, Operators of regular expression and their precedence, Algebraic laws for Regular expressions, Kleen's Theorem, Regular expression to FA, DFA to Regular expression, Arden Theorem, Non Regular Languages, Pumping Lemma for regular Languages. Application of Pumping Lemma, Closure properties of Regular Languages, Decision properties of Regular Languages, FA with output: Moore and Mealy machine, Equivalence of Moore and Mealy Machine, Applications and Limitation of FA.

Unit 3- Context-free languages and pushdown automata: Context-free grammars (CFG) and languages (CFL), Chomsky and Greibach normal forms, nondeterministic pushdown automata (PDA) and equivalence with CFG, parse trees, ambiguity in CFG, pumping lemma for context-free languages, deterministic pushdown automata, closure properties of CFLs.

Unit 4- Context-sensitive languages: Context-sensitive grammars (CSG) and languages, linear bounded automata and equivalence with CSG. Turing machines: The basic model for Turing machines (TM), Turing- recognizable (recursively enumerable) and Turing-decidable (recursive) languages and their closure properties, variants of Turing machines, nondeterministic TMs and equivalence with deterministic TMs, unrestricted grammars and equivalence with Turing machines, TMs as enumerators.

Syllabus

Unit 5- Types of Turing machine: Turing machines and halting Problem

Undecidability: Undecidability, A Language that is Not Recursively Enumerable, An Undecidable Problem That is RE, Undecidable Problems about Turing Machines, Recursive languages, Properties of recursive languages, Post's Correspondence Problem, Modified Post Correspondence problem, Other Undecidable Problems, Counter machines.

TEXTBOOKS:

1. Introduction to Automata Theory, Languages, and Computation, 3nd Edition, John E. Hopcroft, Rajeev Motwani, Jeffrey D. Ullman, Pearson Education.
2. Theory of Computer Science – Automata languages and computation, Mishra and Chandrashekaran, 2nd edition, PHI.

REFERENCE BOOKS:

1. Introduction to Languages and The Theory of Computation, John C Martin, TMH.
2. Introduction to Computer Theory, Daniel I.A. Cohen, John Wiley.
3. A Textbook on Automata Theory, P. K. Srimani, Nasir S. F. B, Cambridge University Press.
4. Introduction to the Theory of Computation, Michael Sipser, 3rd edition, Cengage Learning.
5. Introduction to Formal languages Automata Theory and Computation Kamala Krithivasan, Rama R, Pearson.

Syllabus

DATABASE MANAGEMENT SYSTEMS (CST-011)

L:T:P:: 3:1:0 **Credits-04**

COURSE OBJECTIVES: The objectives of this course are to:

1. Learn the fundamentals of data models and to represent a database system using ER diagrams.
2. Study SQL and relational database design.
3. Understanding the internal storage structures using different file and indexing techniques which will help in physical DB design.
4. Understand the fundamental concepts of transaction processing- concurrency control techniques and recovery procedures.
5. Have the knowledge about the Storage and Query Processing Techniques

COURSE OUTCOMES: On successful completion of the course, the student will be able to:

1. Write relational algebra expressions for that query and optimize the developed expressions.
2. Design the databases using E-R method and normalization.
3. Understand the concepts of function dependencies and various normal forms.
4. Understand the concept of transaction atomicity, consistency, isolation, and durability properties in context of real life examples.
5. Develop the understanding of query processing and advanced databases.

Unit 1-Introduction: Data Abstraction, Data Independence, Data Definition Language(DDL),Data Manipulation Language(DML), 3 level Database System Architecture.
Database models: Entity-relationship model, network model, relational and object oriented data models, integrity constraints, data manipulation operations.

Unit 2-Relational Model: Structure of relational database, Relational Algebra: Fundamental operations, Additional Operations, Extended Relational-Algebra operations, Tuple Relational Calculus – Domain Relational Calculus. SQL: Basic structure, Set operations, Aggregate functions, Null Values, Nested subqueries, Views, Data Definition Language, Embedded SQL, Dynamic SQL, Domain Constraints, Referential Integrity and Triggers.

Unit 3-Relational database design: Functional Dependencies, First, Second, Third Normal Forms, Closure, Armstrong's Axioms, Canonical cover, Decomposition, Properties of Decomposition, Dependency Preservation, Boyce-Codd Normal Form, Fourth Normal Form, Fifth Normal Form.

Unit 4-Transaction processing: Transaction Concepts, ACID Properties, Two-Phase Commit, Save Points, Concurrency Control techniques: Locking Protocols, Two Phase Locking, timestamp-based protocol, Multiversion and optimistic Concurrency Control schemes, Database recovery.

Unit 5-Storage Structure, Query Processing and Advanced database: Storage structures: RAID. File

Syllabus

Organization: Organization of Records, Indexing, Ordered Indices, B+ tree Index Files, B tree Index Files. Query Processing: Overview, Measures of Query Cost, Query optimization. Advanced Database: Object-oriented and object-relational databases, logical databases, web databases, distributed databases, data warehousing and data mining.

TEXTBOOKS:

1. Abraham Silberschatz, Henry F. Korth, S. Sudharshan, ―Database System Concepts, Sixth Edition, Tata McGraw Hill, 2011.

2. RamezElmasri, Shamkant B. Navathe, ―Fundamentals of Database Systems, Sixth Edition, Pearson Education, 2011.

REFERENCE BOOK:

1. C.J.Date, A.Kannan, S.Swamynathan, ―An Introduction to Database Systems, Eighth Edition, Pearson Education, 2006.

2. Raghu Ramakrishnan, ―Database Management Systems, Fourth Edition, McGraw-Hill College Publications, 2015.

3. G.K.Gupta,"Database Management Systems, Tata McGraw Hill, 2011.

Syllabus

UNIVERSAL HUMAN VALUES (AHT-008)

L:T:P:: 2:1:0 **Credits-03**

COURSE OBJECTIVES: The objectives of the course are to:

1. Development of a holistic perspective based on self- exploration about themselves (human being), family, society and nature/existence.
2. Understanding (or developing clarity) of the harmony in the human being, family, society and nature/existence.
3. Strengthening of self-reflection.
4. Development of commitment and courage to act.

COURSE OUTCOMES: On successful completion of the course, the student will be able to:

1. Expected to become more aware of themselves, and their surroundings (family, society, nature)
2. Become more responsible in life, and in handling problems with sustainable solutions, while keeping human relationships and human nature in mind.
3. Have better critical ability.
4. Become sensitive to their commitment towards what they have understood (human values, human relationship and human society).
5. Able to apply what they have learnt to their own self in different day-to- day settings in real life, at least a beginning would be made in this direction.

UNIT 1: Introduction - Value Education
Universal human values; self exploration, natural acceptance an experimental validation; Human aspirations, right understanding, relationship and physical facility, current scenario; Understanding and living in harmony at various levels.

UNIT 2 2: Harmony in the Human Being
Understanding human being, needs of self(I) and body; body as an instrument of 'I'; characteristics and activities of 'I' and harmony in 'I'; harmony of I with the Body: Sanyam and Health, Physical needs an prosperity; Programs to ensure Sanyam and Health.

UNIT 3: Harmony in the Family and Society
Values in human-human relationship; nine universal values in relationships; justice, truth, respect, trust; Difference between intention and competence; Respect and differentiation, Harmony in society: resolution, prosperity, fearlessness and coexistence; Universal harmonious order in society.

UNIT 4: Harmony in the Nature and Existence
Harmony in the nature. Four orders of nature; existence as co-existence, harmony at all levels of existence.

UNIT 5: Harmony in the Professional Ethics
Natural acceptance of human values**,** Definitiveness of Ethical Human Conduct**;** Basis for Humanistic

Syllabus

Education, Humanistic Constitution and Humanistic Universal Order; Competence in professional ethics; Case studies; transition from the present state to Universal Human Order: at individual level and societal level.

TEXT BOOK

1. Human Values and Professional Ethics by R R Gaur, R Sangal, G P Bagaria, Excel Books, New Delhi, 2010

REFERENCE BOOKS

1. Jeevan Vidya: Ek Parichaya, A Nagaraj, Jeevan Vidya Prakashan, Amarkantak, 1999.
2. Human Values, A.N. Tripathi, New Age Intl. Publishers, New Delhi, 2004.
3. The Story of Stuff (Book).
4. The Story of My Experiments with Truth - by Mohandas Karam chand Gandhi.
5. Small is Beautiful - E. F Schumacher.
6. Slow is Beautiful - Cecile Andrews
7. Economy of Permanence - J C Kumarappa
8. Bharat Mein Angreji Raj - PanditSunderlal
9. Rediscovering India - by Dharampal
10. Hind Swaraj or Indian Home Rule - by Mohandas K. Gandhi
11. India Wins Freedom - Maulana Abdul Kalam Azad
12. Vivekananda - Romain Rolland (English)
13. Gandhi - Romain Rolland (English)

Syllabus

COMPUTER ORGANIZATION AND ARCHITECTURE LAB (CSP-007)

L:T:P:: 0:0:2 **Credits-01**

COURSE OBJECTIVES: The objectives of this course are to:

1. Understanding the behaviour of Logic Gates, Adders, Decoders, Multiplexers and Flip-Flops.
2. Understanding the behaviour of ALU, RAM, STACK and PROCESSOR from working modules and the modules designed by the student as part of the experiment.

COURSE OUTCOMES: On successful completion of the course, the student will be able to:

1. Recognize basic logic gates with IC chips.
2. Design combinational circuits using IC Chips.
3. Connect the theory of computer organization with hardware.
4. Implement the concept of adders
5. Apply fundamentals of digital design and extend the learning to design sequential circuits.

LIST OF EXPERIMENTS

1. Implementing HALF ADDER, FULL ADDER using basic logic gates.
2. Implementing Binary -to -Gray, Gray -to -Binary code conversions.
3. Implementing 3-8 line DECODER and Implementing 4x1 and 8x1 MULTIPLEXERS.
4. Verify the excitation tables of various FLIP-FLOPS.
5. Design of an 8-bit Input/ Output system with four 8-bit Internal Registers.
6. Design of an 8-bit ARITHMETIC LOGIC UNIT.
7. Design the data path of a computer from its register transfer language description.
8. Design the control unit of a computer using either hardwiring or microprogramming based on its register transfer language description.
9. Write an algorithm and program to perform matrix multiplication of two n * n matrices on the 2-D mesh SIMD model, Hypercube SIMD Model or multiprocessor system.
10. Study of Scalability for Single board Multi-board, multi-core, multiprocessor using Simulator.

Software Engineering and Agile Practices Lab (CYP-102)

L:T:P:: 0:0:2 **Credits-01**

course objectives:

- To understand the principles and practices of Agile methodologies.
- To apply the Scrum framework in a software development project.
- To set up and implement Continuous Integration and Continuous Deployment pipelines.
- To explore various Agile estimation techniques for project planning.
- To explore and use Agile project management tools.

1. **Introduction to Version Control Systems (VCS):**
    - Set up and configure a version control system (e.g., Git).
    - Create a repository, add files, commit changes, and push to a remote repository.
    - Learn basic Git commands (e.g., git add, git commit, git push, git pull).
2. **Agile Methodologies:**
    - Study and compare different agile methodologies (e.g., Scrum, Kanban, XP).
    - Understand the principles behind agile development and their application in real-world projects.
3. **Scrum Practices:**
    - Simulate a Scrum team environment.
    - Conduct sprint planning, daily stand-ups, sprint reviews, and retrospectives.
    - Use Scrum artifacts like product backlog, sprint backlog, and burndown charts.
4. **Test-Driven Development (TDD):**
    - Learn the principles of TDD.
    - Write unit tests before implementing features.
    - Practice red-green-refactor cycle.
5. **Continuous Integration (CI) and Continuous Deployment (CD):**
    - Set up a CI/CD pipeline using tools like Jenkins, Travis CI, or GitLab CI.
    - Automate the build, test, and deployment process.
    - Understand the benefits of CI/CD in software development.
6. **Pair Programming:**
    - Pair up with a partner and work on a coding task together.
    - Switch roles between the "driver" (writing code) and the "observer" (reviewing and guiding).
    - Reflect on the experience and its impact on productivity and code quality.
7. **Refactoring Techniques:**
    - Identify code smells and refactor code to improve its design and readability.

- Practice common refactoring techniques such as Extract Method, Move Method, and Rename Variable.

8. **Agile Estimation Techniques:**
    - Learn and practice agile estimation techniques like Planning Poker or T-Shirt Sizing.
    - Estimate the effort required for user stories or tasks in a simulated project environment**.**
9. **User Story Mapping:**
    - Create user story maps to visualize the user's journey through the application.
    - Prioritize user stories based on their importance and dependencies.
10. **Retrospective Techniques:**
    - Explore different retrospective formats (e.g., Start-Stop-Continue, 4Ls, Sailboat) and their objectives.
    - Conduct a retrospective session to reflect on the team's performance and identify areas for improvement.
11. **Behavior-Driven Development (BDD):**
    - Understand the principles of BDD and its relationship with agile development.
    - Write acceptance criteria using Given-When-Then format.
    - Implement features based on acceptance criteria.
12. **Agile Metrics and Monitoring:**
    - Identify key metrics to measure the team's performance and project health (e.g., velocity, lead time, cycle time).
    - Set up dashboards to monitor these metrics and track progress over time.

Syllabus

DATABASE MANAGEMENT SYSTEM LAB (CSP-011)

L:T:P:: 0:0:2 **Credits-01**

COURSE OBJECTIVES: The objectives of this course are to

1. Understand data definitions and data manipulation commands.
2. Learn the use of nested and join queries.
3. Understand functions, procedures and procedural extensions of data bases.
4. Familiar with the use of a front-end tool and understand design and implementation of typical database applications

COURSE OUTCOMES: On successful completion of the course, the students will be able to

1. Understand, appreciate, and effectively explain the concepts of database Technologies.
2. Declare and enforce integrity constraints on a database using RDBMS.
3. Devise a complex query using SQL DML/DDL commands.
4. Create views and use in-built functions to query a database.
5. Write PL/SQL programs including stored procedures, stored functions and triggers.

LIST OF EXPERIMENTS

1. Build the following database schemas and perform the manipulation operations on these schemas using SQL DDL,DML,TCL and DCL commands.

(I) Database Schema for a customer-sale scenario

Customer(Custid : integer, cust_name: string)

Item(item_id: integer, item_name: string, price: integer)

Sale(bill_no: integer, bill_data: date, cust_id: integer, item_id: integer, qty_sold: integer)

For the above schema, perform the following:-

a) Create the tables with the appropriate integrity constraint

b) Insert around 10 records in each of the tables

c) List all the bills for the current date with the customer namesand item numbers

d) List the total Bill details with the quantity sold price of theitem and the final amount

e) List the details of the customer who have bought a productwhich has a price>200

f) Give a count of how many products have been bought byeach customer

g) Give a list of products bought by a customer having cust_idas 5

h) List the item details which are sold as of today

i) Create a view which lists out the bill_no, bill_date, cust_id, item_id, price, qty_sold, amount

j) Create a view which lists the date wise daily sales for the last one week

k) Identify the normalization of this schema. Justify your answer.

Syllabus

l) If the schema is not normalized, then normalize the schema.

(II) Database Schema for a Employee-pay scenario

Employee(emp_id : integer, emp_name: string)

Department (dept_id: integer, dept_name:string)

Paydetails(emp_id : integer, dept_id: integer, basic: integer,deductions: integer, additions: integer, DOJ: date)

payroll(emp_id : integer, pay_date: date)

For the above schema, perform the following:—

a) Create the tables with the appropriate integrity constraints

b) Insert around 10 records in each of the tables

c) List the employee details department wise

d) List all the employee names who joined after particular date

e) List the details of employees whose basic salary is between 10,000 and 20,000

f) Give a count of how many employees are working in each department

g) Give a name of the employees whose netsalary>10,000

h) List the details for an employee_id=5

i) Create a view which lists out the emp_name, department, basic, deductions,netsalary

j) Create a view which lists the emp_name and his netsalary

k) Identify the normalization of this schema. Justify your answer

l) If the schema is not normalized then normalize the schema.

2. Construct a PL/SQL program to find largest number from the given three numbers.
3. Build a PL/SQL program to generate all prime numbers below 100.
4. Construct a PL/SQL program to demonstrate %type and %row type attributes.
5. Develop a PL/SQL procedure to find reverse of a given number.
6. Create a PL/SQL procedure to update the salaries of all employees by 10% in their basic pay.
7. Execute a PL/SQL procedure to demonstrate IN, OUT and INOUT parameters.
8. Design a PL/SQL trigger before/after update on employee table for each row/statement.
9. Create a PL/SQL trigger before/after delete on employee table for each row/statement.
10. Build a PL/SQL trigger before/after insert on employee table for each row/statement.
11. Design and build the following applications using SQL and front end tool and generate report
    - Student information system for your college.
    - Hospital Management System.
    - A video library management system.
    - Inventory management system for a hardware / sanitary item shop.

- Banking System.
- Railway Reservation System
- Car Insurance Company

Syllabus

VEER MADHO SINGH BHANDARI UTTARAKHAND TECHNICAL UNIVERSITY

(Formerly Uttarakhand Technical University, Dehradun Established by Uttarakhand State Govt. wide Act no. 415 of 2005)
Suddhowala, PO-Chandanwadi, Premnagar, Dehradun, Uttarakhand (Website- www.uktech.ac.in)

SYLLABUS

For

B. TECH

Cyber Security

3rd Year

Effective From – Session 2024-25

Syllabus

SEMESTER-V													
S. NO.	Subject Codes	Category	Subject	Periods			Evaluation Scheme					Subject Total	Credit
							Sessional Exam			ESE			
				L	T	P	CT	TA	Total	TE	PE		
1	CST-021	DC	Computer Network	3	1	0	30	20	50	100		150	4
2	CYT-106	DC	Risk Management & Analysis	3	1	0	30	20	50	100		150	4
3	CST-023	DC	Operating System	3	1	0	30	20	50	100		150	4
4	CST-010	DC	Design and Analysis of Algorithms	3	1	0	30	20	50	100		150	4
5	CST-012	DC	Compiler Design	3	1	0	30	20	50	100		150	4
6	CYT-107	DC	Application Security	3	1	0	30	20	50	100		150	4
7	CSP-014	DLC	Computer Networks Lab	0	0	2		25	25		25	50	1
8	CYP-103	DC	Application Security lab	0	0	2		25	25		25	50	1
9	CSP-010	DLC	Design and Analysis of Algorithms Lab	0	0	2		25	25		25	50	1
9	CYP-104	DLC	Mini Project-II or Internship-II*	0	0	2			50				1
10	AHT-009	MC	Constitution of India	2	0	0	15	10	25	50			
11	GP-005	NC	General Proficiency						50			50	
			Total	17	3	8						1100	28
	*The Mini Project-II or Internship-II (4-6weeks)will be conducted during summer break after IV semester and will be assessed during the V semester												
	MOOCs course												

Abbreviations: L-No. of Lecture hours per week, **T**-No. of Tutorial hours per week, **P**-No. of Practical hours per week, **CT**-Class Test Marks, **TA**-Marks of teacher's assessment including student's class performance and attendance, **PS**-Practical Sessional Marks, **ESE**-End Semester Examination, **TE**- Theory Examination Marks, PE- Practical External Examination Marks

1 Hr Lecture **1 Hr Tutorial** **2 or 3 Hr Practical**

1 Credit **1 Credit** **1 Credit**

Syllabus

SEMESTER-VI												
S. NO.	Subject Codes	Category	Subject	Periods			Evaluation Scheme					Subject Total	Credit
							Sessional Exam			ESE			
				L	T	P	CT	TA	Total	TE	PE		
1	CYT-108	DC	AI & ML and its impact on Cyber Security	3	1	0	30	20	50	100		150	4
2	CYT-109	DC	Blockchain in Security	3	1	0	30	20	50	100		150	4
3	CYT-110	DC	Ethical Hacking and Penetration Testing	3	1	0	30	20	50	100		150	4
4	CYT-111	DC	IT Systems Security and Physical Security	3	1	0	30	20	50	100		150	4
5	CYT-112	DC	Digital Forensic	3	0	0	30	20	50	100		150	3
6		DE	Departmental Elective-1	3	0	0	30	20	50	100		150	3
7	CYP-105	DLC	Ethical Hacking and Penetration Testing Lab	0	0	2		25	25		25	50	1
8	CYP-106	DLC	AI & ML Lab	0	0	2		25	25		25	50	1
9	CYP-107	DLC	Digital Forensic Lab	0	0	2		25	25		25	50	1
10	CYP-108	DLC	Design Project	0	0	2		25	25	50			1
10	AHT-010	NC	Essence of Indian Traditional Knowledge	2	0	0	15	10	25				
11	GP-006	NC	General Proficiency						50			50	
			Total	17	3	6						1100	26
12													
		DLC	Internship-III/Mini Project-III*	To be completed at the end of the sixth semester (during the Summer).									
	MOOCs course												

Departmental Elective-1		
S. No.	**Subject Code**	**Subject Name**
1	CYT-113	Database Security
2	ITT-113	Ecommerce & Mcommerce
3	CST-027	Web Technology
4	ITT-208	IT LAW & Patent
5	CYT-114	Cyber Law & Cyber Crime
6	CST-035	Cryptography& Network Security

Abbreviations: L-No. of Lecture hours per week, **T**-No. of **CT**-Class Test Marks, **TA**-Marks of teacher's assessment including student's class performance and attendance, **PS**-Practical Sessional Marks, **ESE**-End Semester Examination, **TE**- Theory Examination Marks, PE-Practical External Examination Marks

1 Hr Lecture **1 Hr Tutorial** **2 or 3 Hr Practical**
1 Credit **1 Credit** **1 Credit**

Syllabus

COMPUTER NETWORK (CST-021)

L:T:P:: 3:1:0 **Credits-04**

COURSE OBJECTIVES: The objectives of this course are to

1. Understand the protocol layering and physical level communication.
2. Analyze the performance of a network .and understand the various components required to build different networks.
3. Learn the functions of network layer and the various routing protocols.
4. Familiarize the functions and protocols of the Transport layer.

COURSE OUTCOMES: On completion of the course, the students will be able to

1. Explain the functions of the different layer of the OSI Protocol.
2. Draw the functional block diagram of local area networks (LANs, wide-area networks (WANs) and Wireless LANs (WLANs).
3. Address the issues related to network layer and various routing protocols.
4. Configure DNS, TELNET, EMAIL, File Transfer Protocol (FTP), WWW, HTTP, SNMP.
5. Configure Bluetooth, Firewalls using open source available software and tools.

Unit 1- Data communication Components: Representation of data and its flow Networks, Various Connection Topology, Protocols and Standards, OSI model, Transmission Media, LAN: Wired LAN, Wireless LANs, Connecting LAN and Virtual LAN, Techniques for Bandwidth utilization: Multiplexing - Frequency division, Time division and Wave division, Concepts on spread spectrum.

Unit 2- Data Link Layer and Medium Access Sub Layer: Error Detection and Error Correction - Fundamentals, Block coding, Hamming Distance, CRC; Flow Control and Error control protocols - Stop and Wait, Go back – N ARQ, Selective Repeat ARQ, Sliding Window, Piggybacking, Random Access, Multiple access protocols- Pure ALOHA, Slotted ALOHA, CSMA/CD, CDMA/CA, high level data link control(HDLC), Point To Point protocol (PPP).

Unit 3- Network Layer: Repeater, Hub, Switches, Bridges, Gateways, Switching, Logical addressing – IPV4, IPV6, Address mapping – ARP, RARP, BOOTP and DHCP–Delivery, Forwarding and Unicast Routing protocols.

Unit 4- Transport Layer: Process to Process Communication, User Datagram Protocol (UDP), Transmission Control Protocol (TCP), SCTP Congestion Control; Quality of Service, QoS improving techniques: Leaky Bucket and Token Bucket algorithm.

Unit 5- Application Layer: Domain Name Space (DNS), DDNS, TELNET, EMAIL, File Transfer Protocol (FTP), WWW, HTTP, SNMP, Bluetooth, Firewalls, Basic concepts of Cryptography , Digital Signature.

Syllabus

TEXTBOOK:

1. Behrouz A. Forouzan, Data Communications and Networking, Fifth Edition TMH, 2013.

REFERENCE BOOKS:

1. Larry L. Peterson, Bruce S. Davie, Computer Networks: A Systems Approach, Fifth Edition, Morgan Kaufmann Publishers Inc., 2012.
2. William Stallings, Data and Computer Communications, Tenth Edition, Pearson Education, 2013.
3. Nader F. Mir, Computer and Communication Networks, Second Edition, Prentice Hall, 2014.
4. Ying-Dar Lin, Ren-Hung Hwang and Fred Baker, Computer Networks: An Open Source Approach, McGraw Hill Publisher, 2011.
5. James F. Kurose, Keith W. Ross, Computer Networking, A Top-Down Approach Featuring the Internet, Sixth Edition, Pearson Education, 2013.

Syllabus

RISK MANAGEMENTANALYSIS (CYT-106)

L:T:P:: 3:1:0 **Credits-04**

Course Objective:

1. To provide students with a comprehensive understanding of risk management principles, techniques, and practices
2. To equip students with the skills necessary to identify, assess, and mitigate risks in various organizational contexts.
3. To familiarize students with the tools and methodologies used for risk analysis and decision-making.
4. To enable students to develop effective risk management strategies and policies.
5. To cultivate critical thinking and problem-solving abilities in addressing real-world risk challenges.

Course Outcomes:

1. Understand the fundamental concepts and theories of risk management.
2. Apply risk assessment techniques to identify and evaluate potential risks within an organization.
3. Utilize risk analysis tools such as probability assessment, impact assessment, and risk mapping to quantify and prioritize risks.
4. Develop risk mitigation strategies and contingency plans to minimize the impact of identified risks.
5. Communicate effectively with stakeholders about risk issues, including the presentation of risk reports and recommendations.

Contents		**Hours**
Unit 1	Introduction risk management, elements of Credit Risk, outline and literature, De_nition, market vs. credit Risk, the elements of credit risk: Default, exposure, and loss given default (or recovery), Expected, unexpected loss, andVaR, Credit exposure.	8
Unit 2	Pre-settlement and settlement risk, Measures of exposure, exposure pro_les,Wrong-way and right-way risk, Models of Single Counterparty Default Risk.	6

Syllabus

Unit 3	Risk Management: Introduction to the Theories of Risk Management; The Changing Environment; The Art of Managing Risks	8
Unit 4	The Threat Assessment Process: Threat Assessment and its Input to Risk Assessment; Threat Assessment Method; Example Threat Assessment	8
Unit 5	Vulnerability Issues: Operating System Vulnerabilities; Application Vulnerabilities; Public Domain or Commercial Off-the-Shelf Software; Connectivity and Dependence; Vulnerability assessment for natural disaster, technological hazards, and terrorist threats; implications for emergency response,vulnerability of critical infrastructures;	6

Suggested Readings:

1. "The Basics of Risk Management" by Michel Crouhy, Dan Galai, and Robert Mark
2. "Risk Management: Principles and Practices" by Michael W. Elliotta

Syllabus

OPERATING SYSTEM (CST-023)

L: T:P :: 3:1:0 **Credits-04**

COURSE OBJECTIVES: The objectives of this course are to

1. Learn and understand the Concepts of the operating systems.
2. Learn and understand operating system services.
3. The core structure, functions and design principles of operating system.
4. Interposes communications and basic concepts of virtualization.

COURSE OUTCOMES: On completion of this course, the students will be able to

1. Create processes and threads.
2. Develop process scheduling algorithms for a given CPU utilization specification, Throughput, Turnaround Time, Waiting Time, and Response Time.
3. Develop the techniques for optimally allocating memory to processes by increasing memory utilization and improving access time.
4. Design and implement a file management system.
5. Develop the I/O management functions in OS.

Unit 1- Introduction: Concept of Operating Systems, Generations of Operating systems, Types of Operating Systems, OS Services, System Calls, Structure of an OS -Layered, Microkernel Operating Systems, Concept of Virtual Machine.

Processes: Definition, Process Relationship, Different states of a Process, Process State transitions, Process Control Block (PCB), Context switching Thread: Definition, Various states, Benefits of threads, Types of threads, Concept of multi threads

Unit 2- Process Scheduling: Foundation and Scheduling objectives, Types of Schedulers, Scheduling criteria: CPU utilization, Throughput, Turnaround Time, Waiting Time, Response Time; Scheduling algorithms: Preemptive and Non-preemptive, FCFS, SJF, RR; Multiprocessor scheduling: Real-Time scheduling: RM and EDF.

Inter-process Communication: Critical Section, Race Conditions, Mutual Exclusion, Hardware Solution, Strict Alternation, Peterson's Solution, The Producer-Consumer Problem, Semaphores, Monitors, Message Passing, Classical IPC Problems: Reader's & Writer Problem, Dinning Philosopher Problem etc.

Unit 3- Deadlocks: Definition, Necessary and sufficient conditions for Deadlock, Deadlock Prevention, Deadlock Avoidance: Banker's algorithm, Deadlock detection and Recovery.

Memory Management: Basic concept, Logical and Physical address map, Memory allocation: Contiguous

Syllabus

Memory allocation–Fixed and variable partition– Internal and External fragmentation and Compaction; Paging: Principle of operation – Page allocation –Hardware support for paging, Protection and sharing, Disadvantages of paging.

Unit 4- Virtual Memory: Basics of Virtual Memory – Hardware and control structures – Locality of reference, Page fault, Working Set, Dirty page/Dirty bit – Demand paging, Page Replacement algorithms: Optimal, First in First Out (FIFO), Second Chance (SC), Not recently used (NRU) and Least Recently used(LRU).

Unit 5- File Management: Concept of File, Access methods, File types, File operation, Directory structure, File System structure, Allocation methods (Contiguous, linked, indexed).

Disk Management: Disk structure, Disk scheduling - FCFS, SSTF, SCAN, C-SCAN, Disk reliability.

TEXTBOOKS:

1. AviSilberschatz, Peter Galvin, Greg Gagne , Operating System Concepts Essentials, 9th Edition by, Wiley Asia Student Edition.

2. William Stallings , Operating Systems: Internals and Design Principles, 9th Edition (2022), Prentice Hall of India.

Reference Books:

1. RamazElmasri, A. Gil Carrick, David Levine, ―Operating Systems – A Spiral Approach, Tata McGraw Hill Edition, 2010.

2. Achyut S.Godbole, Atul Kahate, ―Operating Systems, McGraw Hill Education, 2016. 3. Andrew S. Tanenbaum, ―Modern Operating Systems, Second Edition, Pearson Education, 2004.

Syllabus

DESIGN & ANALYSIS OF ALGORITHMS (CST-010)

L:T:P:: 3:1:0 **Credits-04**

COURSE OUTCOMES: The objectives of this course are to:

1. Understand and apply the algorithm analysis techniques.
2. Analyze the efficiency of alternative algorithmic solutions for the same problem.
3. Understand different algorithm design techniques.
4. Understand the limitations of Algorithmic power.

COURSE OUTCOMES: On successful completion of the course, the student will be able to:

1. Analyze worst-case running times of algorithms based on asymptotic analysis and justify the correctness of algorithms.
2. Describe the greedy paradigm and explain when an algorithmic design situation calls for it. For a given problem develop the greedy algorithms.
3. Describe the divide-and-conquer paradigm and explain when an algorithmic design situation calls for it. Synthesize divide-and-conquer algorithms. Derive and solve recurrence relation.
4. Describe the dynamic-programming paradigm and explain when an algorithmic design situation calls for it.
5. Analyze randomized algorithms and approximation algorithms.

Unit 1- Introduction: Characteristics of an algorithm, Analysis of algorithm**:** Asymptotic analysis of complexity bounds – best, average, and worst-case behavior, Sorting techniques and their performance analysis, Time a space trade-off.

Analysis of recursive algorithms through recurrence relations: Substitution method, Recursion tree method and master's theorem.

Unit 2- Fundamental Algorithmic Strategies: Brute-Force, Greedy, Dynamic Programming, Branch- and-Bound and Back tracking methodologies for the design of an algorithms, Illustrations of these techniques for Problem-Solving, Knapsack, Matrix Chain Multiplication, Activity selection and LCS Problem.

Unit 3- Graph and Tree Algorithms: Traversal algorithms: Depth First Search (DFS) and Breadth First Search (BFS), Shortest path algorithms, Minimum Spanning Tree, Topological sorting, Network Flow Algorithm, Binomial Heap and Fibonacci Heap.

Unit 4- Tractable and Intractable Problems: Computability of Algorithms, Computability classes – P, NP, NP-complete and NP-hard, Standard NP-complete problems and Reduction techniques.

Syllabus

Unit 5- Advanced Topics: Approximation algorithms and Randomized algorithms, Distributed Hash Table.

TEXTBOOKS:

1. Thomas H Cormen, Charles E Lieserson, Ronald L Rivest and Clifford Stein, Introduction to Algorithms, 4TH Edition, MITPress/McGraw-Hill.
2. Ellis Horowitz, Sartaj Sahni and SanguthevarRajasekaran, Computer Algorithms/ C++, Second Edition, Universities Press, 2007.

REFERENCE BOOKS:

1. Jon Kleinberg and ÉvaTardos,Algorithm Design, 1ST Edition, Pearson.
2. Michael T Goodrich and Roberto Tamassia,Algorithm Design: Foundations, Analysis, and Internet Examples, Second EditionWiley.
3. Anany Levitin, ―Introduction to the Design and Analysis of Algorithms, Third Edition, Pearson Education, 2012.

Syllabus

COMPILER DESIGN (CST-012)

L:T:P:: 3:1:0 **Credits-04**

COURSE OBJECTIVES: The objectives of this course are to:

1. Learn the various phases of compiler and various parsing techniques.
2. Understand intermediate code generation and run-time environment.
3. Learn to implement front-end of the compiler and code generator.

COURSE OUTCOMES: On successful completion of the course, the student will be able to:

1. Understand the different phases of compiler.
2. Design a lexical analyser for a sample language using LEX tool.
3. Apply different parsing algorithms to develop the parsers for a given grammar using YACC tool.
4. Understand syntax-directed translation and run-time environment.
5. Learn to implement code optimization techniques and a simple code generator.

UNIT - I INTRODUCTION TO COMPILERS: Structure of a compiler – Lexical Analysis – Role of Lexical Analyzer – Input Buffering – Specification of Tokens – Recognition of Tokens – Lex – Finite Automata – Regular Expressions to Automata – Minimizing DFA.

UNIT- II SYNTAX ANALYSIS: Role of Parser – Grammars – Error Handling – Context-free grammars – Writing a grammar – Top Down Parsing - General Strategies, Recursive Descent Parser, Predictive Parser-LL(1) ParserShift Reduce Parser-LR Parser-LR (0)Item Construction of SLR Parsing Table - Introduction to LALR Parser - Error Handling and Recovery in Syntax Analyzer-YACC.

UNIT- III SYNTAX-DIRECTED TRANSLATION: Syntax-Directed Definitions, Evaluation Orders for SDD's, Applications of Syntax-Directed Translation, Syntax-Directed Translation Schemes, Implementing L-Attributed SDD's.

INTERMEDIATE-CODE GENERATION: Variants of Syntax Trees, Three-Address Code, Types and Declarations, Type Checking, Control Flow, Switch-Statements, Intermediate Code for Procedures.

UNIT- IV RUN-TIME ENVIRONMENTS: Stack Allocation of Space, Access to Nonlocal Data on the Stack, Heap Management, Introduction to Garbage Collection, Introduction to Trace-Based Collection.

CODE GENERATION: Issues in the Design of a Code Generator, The Target Language, addresses in the Target Code, Basic Blocks and Flow Graphs, Optimization of Basic Blocks, A Simple Code Generator, Peephole Optimization, Register Allocation and Assignment, Dynamic Programming Code-Generation.

UNIT- V MACHINE-INDEPENDENT OPTIMIZATION: The Principal Sources of Optimization, Introduction to Data-Flow Analysis, Foundations of Data-Flow Analysis, Constant Propagation, Partial-

Redundancy Elimination, Loops in Flow Graphs, peep-hole optimization.

TEXTBOOKS:

1. Compilers Principles, Techniques and Tools, Alfred V. Aho, Ravi Sethi, Jeffrey D. Ullman, PEA.

2. Introduction to Automata Theory Languages & Computation, 3rd Edition, Hopcroft, Ullman, PEA

REFERENCE BOOKS:

1. Theory of Computer Science, Automata Languages and Computation, 2nd Edition, Mishra, Chandra Shekaran, PHI.

2. Elements of Compiler Design, A.Meduna, Auerbach Publications, Taylor and Francis Group

Syllabus

APPLICATION SECURITY (CYT-107)

L:T:P:: 3:1:0 **Credits-04**

Course Objective:

- Understand fundamental principles of application security, including common vulnerabilities and attack vectors.
- Learn various techniques and tools used to identify and mitigate security risks within software applications.
- Gain proficiency in implementing security best practices throughout the software development lifecycle.
- Explore strategies for secure coding, including input validation, authentication, and access control.
- Develop skills in threat modeling and risk assessment to proactively address security concerns in applications.

Course Outcome:

- Ability to recognize and assess security threats and vulnerabilities in software applications.
- Competence in employing industry-standard security measures to protect against common attacks such as SQL injection, cross-site scripting, and session hijacking.
- Proficiency in integrating security practices into the software development process, promoting secure coding habits among development teams.
- Capability to conduct security audits and penetration testing to identify weaknesses and strengthen application security.
- Aptitude to communicate effectively about application security concepts and strategies, both verbally and in written form, to stakeholders across various levels of technical expertise

Contents		Hours
Unit 1	Introduction to hacking Types of hacking, Phases of hacking OS, Types of OS, OS security Kali Linux, Virtualization, Security testing, Blackbox testing, Whitebox testing, Greybox testing	8
Unit 2	SAST, DAST, SSDLC Penetration testing, Information gathering, Port scanning Fingerprint web server, Fingerprint webapplication framework,	6

Syllabus

	Configuration and deployment management testing Enumerate Infrastructure	
Unit 3	HTTP Methods, HTTPS Identity management testing Account enumeration, unenforced username policy Authentication testing - default credentials, weak lockout Authentication testing - bypassing authentication, browser cache weakness Authentication testing - weak password, weak security question Authorization testing - directory traversal Authorization testing - privilege escalation, IDOR	8
Unit 4	Session management testing Cookie attributes, Session variables, Session fixation Session management testing - SSRF, CSRF Session management testing - Session timeout, session puzzling Input validation testing - SQL Injection, Remediation XML Injection, XPath Injection, XSS, Stored XSS, Remediation Http splitting, Remediation, HTTP parameter pollution	8
Unit 5	Cryptography attack, Heartbleed attack Weak SSL/ TLS, Collision Attack Business logic testing - Integrity check, Process limiting. Business logic testing - Circumvention of workflows, Application misuse Client-side testing - CORS, XSS Client-side testing - Java script execution, HTML Injection, Client side URL redirect, Client side testing - Clickjacking, Local storage Vulnerability scanning tools, Reporting.	6

Suggested Readings:

1. The Tangled Web: A Guide to Securing Modern Web Applications" by Michal Zalewski
2. Web Application Security: A Beginner's Guide" by Bryan Sullivan and Vincent Liu

Syllabus

COMPUTER NETWORKS LAB (CSP-014)

L:T:P:: 0:0:2

Credits-01

COURSE OBJECTIVES: The objectives of this course are to

1. Equip the students with a general overview of the concepts and fundamentals of computer networks.
2. Familiarize the students with the standard models for the layered approach to communication between machines in a network and the protocols of the various layers.

COURSE OUTCOMES: On Completion of this course, the students will be able to

1. Learn about hardware component like RJ-45 connector, CAT-6 Cable etc.
2. Implement the various services of data link layer.
3. Configuration of router, hub, switch etc
4. Configuration of server in programming mode they will learn about socket programming, client server programming for deeply understanding TCP/ IP model and various protocols.
5. Configure their own Network management systems in simulation area, they will work on Cisco networking, NS-2 or NS-3 tools for more clear understanding about computer network.

LIST OF PRACTICALS

1. Installation and configuration of NS2 and Qual Net
2. Creating a network: nodes, links and queues, Creating connections, traffic and computing routers Insertion of errors and analysis of trace file.
3. Study of basic network command and network configuration commands.
4. Simple project on NS2 – wired, wireless and combination of wired and wireless
5. Implementation of new protocols in NS2
6. Simulation study of pure ALOHA protocol;
7. Simulation study of slotted ALOHA protocol;
8. Simulation study of Token Bus LAN protocol;
9. Simulation study of Token Ring LAN protocol;
10. Simulation study of WAN protocol like Frame Relay, X. 25
11. Study of 802. 11 wireless LAN protocols.
12. Implement the Distance Vector Routing protocol for finding the shortest path.
13. Write a program to connect server with client and passes information from one system to another and vice versa that by creating / establishing connection.

Syllabus

APPLICATION SECURITY LAB (CYP-103)

L:T:P:: 0:0:2 **Credits-01**

LIST OF EXPERIMENTS:

1. Study of steps to protect your personal computer system by creating User Accounts with Passwords and types of User Accounts for safety and security.
2. Study the steps to protect a Microsoft Word Document of different version with different operating system.
3. Study the steps to remove Passwords from Microsoft Word.
4. Study various methods of protecting and securing databases.
5. Study “How to make strong passwords” and “passwords cracking techniques”.
6. Study the steps to hack a strong password.
7. Implement the SIGNATURE SCHEME – Digital Signature Standard.
8. Demonstrate intrusion detection system (ids) using any tool eg. Snort or any other s/w.
9. Automated Attack and Penetration Tools Exploring N-Stalker, a Vulnerability Assessment Tool
10. Defeating Malware i) Building Trojans ii) Rootkit Hunter

Syllabus

DESIGN & ANALYSIS OF ALGORITHMS LAB (CSP-010)

L:T:P::0:0:2 **CREDIT:01**

COURSE OBJECTIVES: This course's principal objective is to build a solid foundation in algorithms and their applications.

1. To implement various divide and conquer techniques examples.
2. To implement various Greedy techniques examples.
3. To implement various Dynamic Programming techniques examples.
4. To provide a practical exposure of all algorithms.
5. To understand the importance of algorithm and its complexities.

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

1. Solve recurrence equations by considering time and space complexity.
2. Analyze the complexities of various problems in different domains.
3. Solve the problems that comprises of shortest route issue.
4. Solve the problems that address the issue of dynamic programming.
5. Synthesize efficient algorithms in common engineering design situations.

LIST OF EXCERCISES

1. Programming that uses recurrence relations to analyse recursive algorithms.
2. Computing best, average, and worst-case time complexity of various sorting techniques.
3. Performance analysis of different internal and external sorting algorithms with different type of data set.
4. Use of divide and conquer technique to solve some problem that uses two different algorithms for solving small problem.
5. Implementation of different basic computing algorithms like Hash tables, including collision-avoidance strategies, Search trees (AVL and B-trees).
6. Consider the problem of eight queens on an (8x8) chessboard. Two queens are said to attack each otherif they are on the same row, column, or diagonal. Write a program that implements backtracking algorithm to solve the problem i.e. place eight non-attacking queens on the board.
7. Write a program to find the strongly connected components in a digraph.
8. Write a program to implement file compression (and un-compression) using Huffman's algorithm.
9. Write a program to implement dynamic programming algorithm to solve the all pairs shortest path problem.
10. Write a program to solve 0/1 knapsack problem using the following:
    a) Greedy algorithm.
    b) Dynamic programming algorithm.
    c) Backtracking algorithm.
    d) Branch and bound algorithm,
11. Write a program that uses dynamic programming algorithm to solve the optimal binary search tree problem.
12. Write a program for solving traveling salespersons problem using the following:

a) Dynamic programming algorithm.
b) The back tracking algorithm.
c) Branch and bound.

Syllabus

MINI PROJECT-II/ INTERNSHIP-II (CYP-104)

L:T:P:: 0:0:2 **Credits-01**

ABOUT INTERNSHIP/MINI PROJECT

It is an organized method or activity of enhancing and improving engineering students' skill sets and knowledge, which boosts their performance and consequently helps them meet their career objectives. Industrial Training is essential in developing the practical and professional skills required for an Engineer and an aid to prospective employment.

OBJECTIVES OF INTERNSHIP/MINI PROJECT:

1. The main objective of the internship/mini projectis to expose the students to the actual working environment and enhance their knowledge and skill from what they have learned in college.
2. Another purpose of this program is to enhance the good qualities of integrity, responsibility, and self-confidence. Students must follow all ethical values and good working practices.
3. It is also to help the students with the safety practices and regulations inside the industry and to instils the spirit of teamwork and good relationship between students and employees.

COURSE OUTCOMES: At the end of internship/mini project, the students will be able to

1. Understand organizational issues and their impact on the organization and employees.
2. Identify industrial problems and suggest possible solutions.
3. Relate, apply and adapt relevant knowledge, concepts and theories within an industrial organization, practice and ethics.
4. Apply technical knowledge in an industry to solve real world problems.
5. Demonstrate effective group communication, presentation, self-management, and report writing skills**.**

Syllabus

CONSTITUTION OF INDIA (AHT-009)

L:T:P:: 2:0:0 **Credits-0**

COURSE OBJECTIVES: The objectives of this course are to

1. To acquaint the students with legacies of constitutional development in India and help to understand the most diversified legal document of India and philosophy behind it.
2. To make students aware of the theoretical and functional aspects of the Indian Parliamentary System.
3. To channelize students' thinking towards basic understanding of the legal concepts and its implications for engineers.

COURSE OUTCOMES

On successful completion of the course, the students will be able to

1. Understand the basic knowledge and salient features of Indian Constitution.
2. Identify and explore the basic features and modalities about Indian constitution.
3. Discusses the essence of Union and its territories, Citizenship, Fundamental Rights, DPSP and Fundamental Duties.
4. Differentiate and relate the functioning of Indian parliamentary system at the center and state level.
5. Differentiate different aspects of Indian Legal System and its related bodies.

Unit-1 Constitutional Framework

Meaning of Terms and Phrases frequently used in political system like constitution, constitutionalism, Rule of Law, Federal system, Government and so on. Historical Background of Indian Constitution, Making of Indian Constitution, Salient features of Indian Constitution, Preamble of Indian Constitution.

Unit-2 Different Parts, Articles, and their significance

Part I to IVA (Union and its territories w.r.t. Indian States, Citizenship, Fundamental Rights conferred to citizens and foreigners, Directive Principles of State Policy– Its importance and implementation and Fundamental Duties and its legal status), Article 1 to 51A and their significance.

Unit-3 System of Government

Parliamentary Form of Government in India – The constitution powers and status of the President of India, Federal structure and distribution of legislative and financial powers between the Union and the States, Emergency Provisions: National Emergency, President Rule, Financial Emergency and Amendment of the Constitutional Powers and Procedure and the significance of basic structure in Indian Judicial system

Unit-4 Working of Central, State & Local Self Government as per constitution

Framework for central government (President, Vice president, Prime Minister, Central council of

ministers, Parliament, Supreme court and so on), Framework for state government (Governor, Chief Minister, state legislature, High court and so on) and Framework for local self government (Panchayatiraj, Municipalities) and Union Territories.

Unit-5 Constitutional, Non-Constitutional and other bodies

Discussion on Various constitutional bodies like Election Commission, UPSC, SPSC, Finance commission, NCSC, NCST, NCBC, CAG and AGI. Discussion on Various non-constitutional bodies like NITI Aayog, NHRC, CIC, CVC, CBI, Lokpal and Lokayukta. Discussion on Various other constitutional bodies like Co- operative societies, Official Language, Tribunals etc.

Text/Reference books-

1. M. Laxmikanth, "Indian Polity", McGraw- Hill, 6th edition, 2020
2. D.D. Basu, "Introduction to the Indian Constitution", LexisNexis, 21st edition, 2020
3. S.C. Kashyap, " Constitution of India", Vitasta publishing Pvt. Ltd., 2019

Syllabus

AI &ML and its impact on Cyber Security (CYT - 108)

L:T:P:3:1:0 **CREDIT:04**

Course Description: This course explores the intersection of artificial intelligence (AI) and machine learning (ML) with cybersecurity. Students will learn how AI and ML technologies are transforming cybersecurity practices, both defensively and offensively. Topics include AI-driven threat detection, adversarial ML, automated attack techniques, and the ethical considerations of AI in cybersecurity.

Prerequisites: Basic understanding of cybersecurity concepts and familiarity with programming languages such as Python.

Course Objectives:

- Understand the fundamental principles of artificial intelligence and machine learning.
- Explore how AI and ML technologies are applied in cybersecurity for threat detection, anomaly detection, and attack prediction.
- Examine the challenges and limitations of AI & ML in cybersecurity, including adversarial attacks and model vulnerabilities.
- Analyze real-world case studies and examples of AI & ML applications in cybersecurity.
- Discuss the ethical considerations and implications of using AI & ML in cybersecurity.

Contents		Hrs
Unit 1	**AI and ML in threat detection and Machine Learning Techniques for Threat Detection** ▪ Supervised learning for Threat Detection ▪ Unsupervised Learning for threat detection ▪ Semi-supervised Learning for threat detection ▪ Deep Learning Techniques for Threat Detection ▪ Convolutional Neural Networks (CNNs) for threat detection ▪ Recurrent Neural Networks (RNNs) for threat detection ▪ Generative Adversarial Networks (GANs) for threat detection ▪ Use Cases of AI and ML in Threat Detection ▪ Network traffic analysis using AI and ML	6

	▪ Malware detection using AI and ML ▪ Intrusion detection using AI and ML ▪ Challenges and Limitations of AI and ML in Threat Detection ▪ Data quality and quantity challenges ▪ Security and privacy considerations ▪ Explainability and interpretability challenges ▪ Future of AI and ML in Threat Detection ▪ Emerging trends in AI and ML for threat detection ▪ Future challenges and opportunities	
Unit 2	**AI and ML in vulnerability assessment and AI and ML in network security** ➢ Introduction ➢ Machine Learning Techniques for vulnerability assessment &network security ➢ Deep Learning Techniques for vulnerability assessment &network security ➢ Use Cases of AI and ML in Vulnerability Assessment &Network Security ▪ Vulnerability detection using AI and ML ▪ Network security monitoring using AI and ML ▪ Threat intelligence using AI and ML ➢ Challenges &Limitations of AI and ML in Vulnerability Assessment& Network Security ▪ Data quality and quantity challenges ▪ Security and privacy considerations ▪ Explain ability and interpretability challenges ➢ Future of AI and ML in vulnerability assessment and network security	6
Unit 3	**AI and ML in access control and AI and ML in incident response** ➢ Introduction ➢ Machine Learning Techniques for vulnerability assessment and incident response ➢ Deep Learning Techniques for vulnerability assessment and incident response ➢ Use Cases of AI and ML in Access Control and Incident Response ▪ User behavior analytics using AI and ML ▪ Authentication and authorization using AI and ML ▪ Threat hunting and detection using AI and ML ▪ Challenges and Limitations of AI and ML in Access Control and Incident Response ▪ Data quality and quantity challenges ▪ Security and privacy considerations ▪ Explain ability and interpretability challenges. ▪ Future of AI and ML in access control and incident	6

Syllabus

	response	
Unit 4	**AI and ML in compliance and AI and ML in fraud detection** ➢ Introduction ➢ Machine Learning Techniques for compliance and fraud detection ➢ Deep Learning Techniques for compliance and fraud detection ➢ Use Cases of AI and ML in Compliance and Fraud Detection ▪ Regulatory compliance using AI and ML ▪ Fraud detection and prevention using AI and ML ▪ Anti-money laundering (AML) and Know Your Customer (KYC) using AI and ML ▪ Challenges and Limitations of AI and ML in Compliance and Fraud Detection ▪ Data quality and quantity challenges ▪ Security and privacy considerations ▪ Explainability and interpretability challenges Future of AI and ML in compliance and fraud detection	6
Unit 5	**AI and ML in data protection** ➢ Introduction ➢ Machine Learning Techniques for compliance ➢ Deep Learning Techniques for compliance ➢ Use Cases of AI and ML in Data Protection ▪ Data loss prevention (DLP) using AI and ML ▪ Data classification and labeling using AI and ML ▪ Anomaly detection and prevention using AI and ML ▪ Challenges and Limitations of AI and ML in Data Protection ▪ Data quality and quantity challenges ▪ Security and privacy considerations ▪ Explainability and interpretability challenges ➢ Future of AI and ML in data protection	6

Suggested Readings:

1.Artificial Intelligence and Cybersecurity" by Terrence August and Andrew Marrington.
2.Machine Learning and Security" by Mark Stamp
3.Data Mining and Machine Learning in Cybersecurity" by Sumeet Dua and Xian Du
4.Machine Learning and Security: Protecting Systems with Data and Algorithms" by Clarence Chio and David Freeman
5.Applied Artificial Intelligence for Cyber Security" by Dietmar Jannach and Peter Kieseberg.

Syllabus

BLOCKCHAIN IN SECURITY (CYT-109)

L:T:P:: 3:1:0 **Credits-04**

Course Description:

This course explores the intersection of blockchain technology and cybersecurity. Students will learn the fundamentals of blockchain, its security features, and its applications in cybersecurity. Topics include distributed ledger technology, cryptographic principles, smart contracts, and decentralized identity management.

Prerequisites:

Basic understanding of cybersecurity concepts and familiarity with computer networks and cryptography.

Unit 1: Introduction to Blockchain Technology

Overview of distributed ledger technology, Fundamentals of blockchain architecture and components, Cryptographic principles in blockchain: hash functions, digital signatures, and cryptographic hash functions

Unit 2: Blockchain Security Fundamentals

Security features of blockchain: immutability, transparency, and decentralization,Consensus mechanisms: Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerance (BFT),Securing blockchain networks: network security, node authentication, and data integrity

Unit 3: Smart Contracts and Decentralized Applications (DApps)

Introduction to smart contracts and their security implications,Design principles for secure smart contracts,Decentralized application development and security considerations

Unit 4: Blockchain for Data Security

Secure data storage and sharing using blockchain,Data integrity and provenance with blockchain technology,Blockchain-based authentication and access control mechanisms

Unit 5: Blockchain for Identity Management

Identity management challenges in the digital age,Decentralized identity solutions using blockchain,Self-sovereign identity and privacy-preserving authentication

Textbook:

1. "Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications" by Imran Bashir

Syllabus

ETHICAL HACKING AND PENETRATION TESTING (CYT-110)

L:T:P:3:1:0 **CREDIT:04**

Course Objectives:

1. to describe the fundamental concepts of protecting a network from attacks.
2. to enumerate the techniques for collecting the network and the host information by a remote user.
3. to learn the techniques by which the adversary can discover and do mapping of systems, can orchestrate unauthorized manipulation of data, disable network systems or services and deny access to resources by legitimate users.
4. to analyse the techniques used by the adversary to detect the common vulnerabilities.
5. to apply the knowledge gained to protect the network as well as the host systems from the adversary attacks.

Course Outcomes: students will

1. have a knowledge of the basic concepts of network, host, services and vulnerability gathering techniques employed by an attacker.
2. be able to use the tools for doing network foot printing including stealth scanning.
3. be able to analyze the installations for the vulnerabilities that could be exploited by an adversary.
4. be able to design the secure system installations that can withstand the adversarial attacks.
5. be able to extend the existing tools for network and systems protection.

UNIT-1: INTRODUCTION

Review of the Network Fundamentals, Network Topologies, Network Components, TCP/IP Networking Basics, TCP/IP Protocol Stack: DNS, SNMP, TCP, UDP, IP, ARP, RARP, ICMP protocols. Ethernet, Subnet Masking, Subnetting, Supernetting. Review of the Security Basics: Attributes, Mechanisms and Attacks Taxonomy. The CIA Traid. Threats, Vulnerabilities, Attacks

UNIT-2: NETWORK SECURITY CONCERNS

Network Security Concerns. Fundamental Network Security Threats. Types of Network Security Threats. Network Security Vulnerabilities, their types: Technological Vulnerabilities, Configuration Vulnerabilities, Security policy Vulnerabilities. Types of Network Security Attacks

UNIT-3: INTELLIGENCE (INT) GATHERING

Learning about the target, its business, its organizational structure, and its business partners. To output the list of company names, partner organization names, and DNS names, and the servers. The concepts of Search engines, Financial databases, Business reports. The use of WHOIS, RWHOIS, Domain name registries and registrars, Web archives and the corresponding open source tools for mining these data. Cloud reconnaissance.

UNIT-4: NETWORK FOOTPRINTING

Active & Passive Footprinting. Network and system footprinting. Tools for network footprinting. Using Search

engines to find the tools. Mining the DNS host names, corresponding IP addresses, IP address ranges, Firewalls, Network maps. Use of search engines, social media, social engineering, the websites of the target organization. Using archive.org. Using Neo trace, DNS Footprinting and whois databases. Use of the contemporary tools (e.g. png, port scanners) for finding these information. Email footprinting. Email Tracking. Footprinting through Google tools. Using traceroute. Verification to confirm the validity of information collected in the prior phases. The countermeasures to prevent successful network footprinting.

UNIT-5:SCANNING & ENUMERATION:

Scanning: goals and type, overall scanning tips, sniffing with tcpdump, network tracing, port scanning. OS fingerprinting, version scanning. Identify open ports. Web Service Review Tools: Identify web-based vulnerabilities. Network Vulnerability Scanning Tools: Identify infrastructure-related security issues. The illustrative tools are Nmap, ping, AngryIP, Nikto, OpenVAS, udp-proto-scanner, Netsparker, Nessus, Masscan, SQLMap, Nexpose, Burpsuite, Qualys, HCL AppScan, Amass, wpscan, Eyewitness, WebInspect, ZAP. Stealth Scannning: Scanning Beyond an IDS. Network diagram generation using typical tools viz. Network Topology Mapper, OpManager, LANState, Friendly Pinger. Proxy Servers, The Onion Routing. http tunneling. ssh tunneling. Anonymizers.

UNIT-6: EXPLOITATION

Network based exploitation: using tools a such as Metasploit to compromise vulnerable systems, basics of pivoting, and pilfering. Detection of IP Spoofing. Common web vulnerabilities: Cross-site scripting, OS and Command injections, Buffer overflows, SQL injection, race conditions, and such other vulnerabilities scanning and exploitation techniques, including those in OWASP Top 25. Extracting information about the user names using email IDs, the list of default passwords used by the products used at the target, user names using the SNMP protocol, user groups from Windows and the DNS zone transfer information. SuperScan. Route Analysis Tools. SNMP Enumeration. Reconnaissance Attacks and how to mitigate reconnaissance attacks.

BOOKS RECOMMENDED

1. John Slavio. Hacking: A Beginners' Guide to Computer Hacking, Basic Security, And Penetration Testing.

2. Yuri Diogenes, Dr. Erdal Ozkaya. Cybersecurity – Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals, 2nd Edition Kindle Edition, Packt Publishing; 2nd edition, 2019.

3. Hidaia Mahmood Alassouli. Footprinting, Reconnaissance, Scanning and Enumeration Techniques of Computer Networks, Blurb Publishers.

4. Robert Shimonski. Cyber Reconnaissance, Surveillance and Defense 1st Edition, Kindle Edition, Syngress;

2014.

5. by Format: Kindle EditionMichael Sikorski, Andrew Honig. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software

6. Dafydd Stuttard and Marcus Pinto. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws

Syllabus

IT Systems Security and Physical Security (CYT-111)

L:T:P:: 3:1:0 **Credits-04**

Course Objectives:

The purpose of this course is to provide understanding of the main issues related to security in modern networked computer systems. This covers underlying concepts and foundations of computer security, basic knowledge about security-relevant decisions in designing IT infrastructures, techniques to secure complex systems and practical skills in managing a range of systems, from personal laptop to large-scale infrastructures.

Course Outcomes:

On completion of this course, students should have gained a good understanding of the concepts and foundations of computer security, and identify vulnerabilities of IT systems. The students can use basic security tools to enhance system security and can develop basic security enhancements in stand-alone applications.

Syllabus:

UNIT 1

Computer Security Concepts- Introduction to Information Security, Introduction to Data and Network Security, Integrity, and Availability, NIST FIPS 199 Standard, Assets and Threat Models

UNIT 2

Control Hijacking– Attacks and defenses, Buffer overflow and control hijacking attacks Exploitation techniques and fuzzing- Finding vulnerabilities and exploits Dealing with Legacy code- Dealing with bad (legacy) application code: Sandboxing and Isolation. Least privilege, access control, operating system security- The principle of least privilege, Access control concepts, Operating system mechanisms, Unix, Windows, Qmail, Chromium, and Android examples.

UNIT 3

Basic web security model- Browser content, Document object model (DOM), Same-origin policy. Web Application Security- SQL injection, Cross-site request forgery, Cross-site scripting, Attacks and Defenses, Generating and storing session tokens, Authenticating users, The SSL protocol, The lock icon, User interface attacks, Pretty Good Privacy.

UNIT 5

Network Protocols and Vulnerabilities- Overview of basic networking infrastructure and network protocols, IP, TCP, Routing protocols, DNS. Network Defenses- Network defense tools, Secure protocols, Firewalls, VPNs, Tor, I2P, Intrusion Detection and filters, Host-Based IDS vs Network-Based IDS, Dealing with unwanted traffic: Denial of service attacks. Malicious Software and Software Security- Malicious Web, Internet Security Issues, Types of Internet Security Issues, Computer viruses, Spyware, Key-Loggers, Secure Coding, Electronic and Information Warfare. Mobile platform security models- Android, iOSMobile platform security models, Detecting Android malware in Android markets.

UNIT 6

Security Risk Management- How Much Security Do You Really Need, Risk Management, Information Security Risk Assessment: Introduction, Information Security Risk Assessment: Case Studies, Risk Assessment in Practice. The Trusted Computing Architecture- Introduction to Trusted Computing, TPM Provisioning, Exact Mechanics of TPM.

Text books and References:

1. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th edition, 2010.

2. Michael T. Goodrich and Roberto Tamassia, Introduction to Computer Security, Addison Wesley, 2011.
3. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th edition, 2010.
4. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 2001.

Syllabus

DIGITAL FORENSIC (CYT-112)

L:T:P:3:0:0 **CREDIT:03**

COURSE OBJECTIVES:

1. Provides an in-depth study of the rapidly changing and fascinating field of computer forensics.
2. Combines both the technical expertise and the knowledge required to investigate, detect and prevent digital crimes.
3. Understand how to manage Evidence & Presentation
4. Knowledge on digital forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation, e-discovery tools E-evidence collection and preservation, investigating operating systems and file systems, network forensics, art of steganography and mobile device forensics.
5. To gain knowledge on Mobile Forensics.

COURSE OUTCOMES:

1. Understand relevant legislation and codes of ethics.
2. Investigate computer forensics and digital detective and various processes, policies and procedures data acquisition and validation, e-discovery tools.
3. Analyze E-discovery, guidelines and standards, E-evidence, tools and environment.
4. Apply the underlying principles of Email, web and network forensics to handle real life problems
5. Use IT Acts and apply mobile forensics techniques.

Course Content:-

UNIT - I

Digital Forensics Science: Forensics science, computer forensics, and digital forensics. Computer Crime: Criminalistics as it relates to the investigative process, analysis of cybercriminalistics area, holistic approach to cyber-forensics.

UNIT - II

Cyber Crime Scene Analysis: Discuss the various court orders etc., methods to search and seizure electronic evidence, retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation.

UNIT - III

Evidence Management & Presentation: Create and manage shared folders using operating system, importance of the forensic mindset, define the workload of law enforcement, Explain what the normal case would look like, Define who should be notified of a crime, parts of gathering evidence, define and apply probable cause.

Syllabus

UNIT - IV

Computer Forensics: Prepare a case, Begin an investigation, Understand computer forensics workstations and software, Conduct an investigation, Complete a case, Critique a case. Network Forensics: open-source security tools for network forensic analysis, requirements for preservation of network data

UNIT - V

Mobile Forensics: mobile forensics techniques, mobile forensics tools. Legal Aspects of Digital Forensics: IT Act 2000, amendment of IT Act 2008. Recent trends in mobile forensic technique and methods to search and seizure electronic evidence.

TEXT BOOKS:

1. B. Nelson, A. Phillips, and C. Steuart, Guide to Computer Forensics and Investigations, 4th Edition, Course Technology, 2010

REFERENCE BOOKS:

1. John Sammons, The Basics of Digital Forensics, 2nd Edition, Elsevier, 2014
2. John Vacca, Computer Forensics: Computer Crime Scene Investigation, 2nd Edition, Laxmi Publications, 2005.

Syllabus

DEPARTMENTAL ELECTIVE-1

DATABASE SECURITY (CYT-113)

L:T:P:3:0:0 **CREDIT:03**

COURSE OBJECTIVES:

1. Give an Overview of information security
2. Give an overview of Access control of relational databases
3. To learn the security of databases
4. To learn the design techniques of database security
5. To learn the secure software design

COURSE OUTCOMES: Students should be able to

1.Understand the Web architecture and applications

2.Understand client side and service side programming

3.Understand how common mistakes can be bypassed and exploit the application

4.Identify common application vulnerabilities.

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.

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.

Syllabus

DEPARTMENTAL ELECTIVE-1

E-COMMERCE AND M-COMMERCE (ITT-113)

L:T:P:: 3:0:0 **Credits-03**

COURSE OBJECTIVES:

1. To provide students with an overview and understanding of e-commerce with a specific emphasis on Internet Marketing.
2. To explore the major issues associated with e-commerce-security, privacy, intellectual property rights, authentication, encryption, acceptable use policies, and legal liabilities.

COURSE OUTCOMES:

1. Obtain a general understanding of basic business management concepts.
2. Have complete knowledge about basic technical concepts relating to E-Commerce.
3. Obtain thorough understanding about the security issues, threats and challenges of E-Commerce.

UNIT - I

History of E-commerce and Indian Business Context: E-Commerce –Emergence of the Internet – Emergence of the WWW – Advantages of E-Commerce – Transition to E-Commerce in India – The Internet and India – E-transition Challenges for Indian Corporate. Business Models for Ecommerce: Business Model – E-business Models Based on the Relationship of Transaction Parties - E-business Models Based on the Relationship of Transaction Types.

UNIT - II

Enabling Technologies of the World Wide Web: World Wide Web – Internet Client-Server Applications – Networks and Internets – Software Agents – Internet Standards and Specifications – ISP. e-Marketing :Traditional Marketing – Identifying Web Presence Goals – Online Marketing – E-advertising – E-branding.

UNIT - III

E-Security: Information system Security – Security on the Internet – E-business Risk Management Issues – Information Security Environment in India. Legal and Ethical Issues : Cybers talking – Privacy is at Risk in the Internet Age – Phishing – Application Fraud – Skimming – Copyright – Internet Gambling – Threats to Children.

UNIT - IV

e-Payment Systems: Main Concerns in Internet Banking – Digital Payment Requirements – Digital Token-based

e-payment Systems – Classification of New Payment Systems – Properties of Electronic Cash – Cheque Payment Systems on the Internet – Risk and e-Payment Systems – Designing e-payment Systems – Digital Signature – Online Financial Services in India – Online Stock Trading.

UNIT - V

Information systems for Mobile Commerce: What is Mobile Commerce? – Wireless Applications –Cellular Network – Wireless Spectrum – Technologies for Mobile Commerce – Wireless Technologies –Different Generations in Wireless Communication – Security Issues Pertaining to Cellular Technology. Portals for E-Business: Portals – Human Resource Management – Various HRIS Modules.

TEXT BOOK:

1. P.T.Joseph, S.J., “E-Commerce - An Indian Perspective”, PHI 2012, 4th Edition.

REFERENCE BOOKS:

1. David Whiteley , “E-Commerce Strategy, Technologies and Applications”, Tata McGraw Hill, 2001.
2. Ravi Kalakota, Andrew B Whinston, “Frontiers of Electronic Commerce”, Pearson 2006, 12th Impression.

WEB REFERENCES:

- https://www.docsity.com/en/e-commerce-notes-pdf-lecture-notes-universitylevel/2484734/
- https://magnetoitsolutions.com/blog/advantages-and-disadvantages-of-ecommerce
- https://www.researchgate.net/publication/320547139ECommerce_Merits_and_Demerits_A_Review_Pp

Syllabus

DEPARTMENTAL ELECTIVE-1

WEB TECHNOLOGY (CST-027)

L:T:P:: 3:0:0 **Credits-03**

COURSE OBJECTIVES: The objectives of this course are to

1. Understand about client-server communication and protocols used during communication.
2. Design interactive web pages using Scripting languages.
3. Learn server-side programming using servlets and JSP.
4. Develop web pages using XML/XSLT.

COURSE OUTCOMES: On successful completion of this course, the student will be able to:

1. Design simple web pages using mark-up languages like HTML and XHTML.
2. Create dynamic web pages using DHTML and java script that is easy to navigate and use.
3. Program server-side web pages that have to process request from client side web pages.
4. Represent web data using XML and develop web pages using JSP.
5. Understand various web services and how these web services interact.

UNIT-I Introduction to HTML: HTML Common tags- List, Tables, images, forms, Frames; Cascading Style sheets; Introduction to JavaScript: Scripts, Objects in Java Script, Dynamic HTML with Java Script XML: Document type definition, XML Schemas, Document Object model, Presenting XML, Using XML Processors: DOM and SAX

UNIT-II Java Beans: Introduction to Java Beans, Advantages of Java Beans, BDK Introspection, Using Bound properties, Bean Info Interface, Constrained properties Persistence, Customizes, Java Beans API, Introduction to EJB's

UNIT-III Web Servers and Servlets: Tomcat web server, Introduction to Servelets: Lifecycle of a Serverlet, JSDK, The Servelet API, Thejavax.servelet Package, Reading Servelet parameters, Reading Initialization parameters. The javax.servelet HTTP package, Handling Http Request & Responses, Using Cookies-Session Tracking, Security Issues.

UNIT-IV Introduction to JSP: The Problem with Servelet. The Anatomy of a JSP Page, JSP Processing. JSP Application Design with MVC Setting Up and JSP Environment: Installing the Java Software Development Kit, Tomcat Server & Testing Tomcat

UNIT-V JSP Application Development: Generating Dynamic Content, Using Scripting Elements Implicit JSP Objects, Conditional Processing – Displaying Values Using an Expression to Set an Attribute, Declaring Variables and Methods Error Handling and Debugging Sharing Data Between JSP pages, Requests, and Users Passing

Control and Date between Pages – Sharing Session and Application Data – Memory Usage Considerations.

TEXT BOOK:

1. Jeffrey C. Jackson, "Web Technologies--A Computer Science Perspective", Pearson Education, 2006.

REFERENCE BOOK:

1. Robert. W. Sebesta, "Programming the World Wide Web", 8thEdition(2022), Pearson Education, 2007.

2. Deitel, Deitel, Goldberg, "Internet & World Wide Web How To Program", Third Edition, Pearson Education, 2006.

3. Marty Hall and Larry Brown, Core Web Programming Second Edition, ‖ ‖ Volume I and II, Pearson Education, 2001.

4. Bates, ―Developing Web Applications‖, Wiley, 2006

Syllabus

DEPARTMENTAL ELECTIVE-1

IT LAWS AND PATENTS (ITT-208)

L:T:P:: 3:0:0 **CREDITS-03**

Course Objectives:

1. The course aims at acquainting the students with the Basic concepts of Technology and Law and also puts those concepts in their practical perspective. It also provides an elementary understanding of the authorities under IT Act as well as penalties and offences under IT Act.

2. The course aims at providing extensive knowledge regarding IT Act, 2000 and Cyber Space Jurisdiction to the students so that students do not face any difficulty while handling practical cases in future as an advocate.

3. The course aims at acquainting the students with Cyber Crime & Computer related Crimes and also freedom of speech in cyber space. It also provides an elementary understanding of the Indian Penal Law and Cyber Crimes.

Course Outcomes:

1. Give Learners In Depth Knowledge Of Information Technology Act And Legal Frame Work Of Right To Privacy, Data Security And Data Protection.

2. To develop the conceptual understanding of the cyber dispute and its resolution

3.To explain the regime of the cyber laws

UNIT 1

Evolution of the Information Technology Act, Genesis and Necessity: International Perspective, History of Cyber law in India, Salient features of the Information Technology Act, 2000: Various concepts (Definitions), Digital Signature,Electronic Governance,Attribution, Acknowledgement and Despatch of Electronic Records., Secure Electronic Records and Secure Digital Signatures, Regulation of Certifying Authorities, Digital Signature Certificates,Duties of Subscribers.

UNIT 2

Penalties and Adjudication, The Cyber Regulations Appellate Tribunal, Offences, Network Service providers not to be liable in certain cases, Miscellaneous-Various Government Initiatives for awareness,The Information Technology (Amendment) Bill, 2006

UNIT 3

Impact of other related Acts (Amendments) - a. Amendments to Indian Penal Code. b. Amendments to Criminal Procedure Code. c. Amendments to Indian Evidence Act. d. Amendments to Bankers Books Evidence Act. e. Amendments to Reserve Bank of India Act, The Information Technology (Certifying Authorities) rules, 2001., The Cyber Regulations appellate Tribunals (Procedure) rules, 2000,The Information Technology (Certifying Authorities) regulations, 2001, The Cyber regulations appellate tribunal (Procedure for investigation of misbehaviour of incapacity of presiding officer) Rules, 2003,The Information Technology (Qualification and Experience of Adjudicating officers and manner of holding enquiry) Rules, 2003. a. Performa for complain to the

adjudicating officer,The Information Technology (use of electronic record and digital signatures)Rules, 2004,The Information Technology (Security procedure)Rules, 2004

UNIT 4

Concept of Patent – Historical view of Patent system in India and International Scenario – Evolution of Patent Laws in India – Legal basis of Patent Protection. Patentable Inventions - Process and Product (Biotechnology / Pharmaceutical Products / Software programme) – Patent protection of computer programme – Inventions NOT patentable.

UNIT 5

Process of Obtaining a Patent – Application- Examination – Acceptance - Opposition – Sealing of Patents – Preservation of Patents- Documentation – Register of Patents. Duration of Patents – Rights of Patentee – Limitation of rights - Use and exercise of Rights – Right to Secrecy – Compulsory Licenses – Special Categories

Reference books:

1. Raj, Niharikia, Law & Technology, Universal Law Publishing. Information Technology Act, 2000.

2. Fisher, Matthew (ed.), Fundamentals of Patent Law: Interpretation and Scope of Protection, (2010), New Delhi, Mohan law House.

3. Miller, Joseph Scott (ed.), Patents, (2010), UK, Edward Elgar.

4. Kankanala, Kalyan C., Indian Patent Law and Practice, (2010), India, Oxford University Press

5. Dr. Bhandari, M.K. Law relating to IPR, Central Law Publication, (4th Edition 2015)

Syllabus

DEPARTMENTAL ELECTIVE-1

Cyber Law and Cyber Crime (CYT-114)

L:T:P:: 3:0:0 **Credits-03**

Course Objectives:

- Understand the legal framework surrounding cyberspace, including laws, regulations, and international treaties governing cyber activities.
- Explore various types of cyber crimes, including hacking, phishing, identity theft, and cyberterrorism, and understand their legal implications.
- Analyze case studies and real-world examples of cyber incidents to understand the legal challenges and responses in addressing cyber threats.
- Develop critical thinking and problem-solving skills to navigate complex legal issues in cyberspace and formulate strategies for preventing and combating cyber crimes.

Course Outcomes:

- Students will demonstrate a comprehensive understanding of cyber laws and regulations, including their historical context, scope, and enforcement mechanisms.
- Students will be able to identify different types of cyber crimes, analyze their impact on individuals, organizations, and society, and assess the legal strategies for addressing them.
- Students will develop the ability to interpret and apply cyber laws in practical scenarios, such as investigating cyber incidents, prosecuting cyber criminals, and protecting digital assets.
- Students will acquire the knowledge and skills needed to contribute to the development of effective cyber security policies, legal frameworks, and compliance standards.

Course Description:

This course provides an in-depth examination of cyber law and cybercrime, focusing on legal frameworks, regulations, and enforcement mechanisms related to cybersecurity. Students will explore various types of cybercrimes, legal challenges in prosecuting cyber offenders, and strategies for combating cyber threats.

Unit 1: Introduction to Cyber Law and Legal Frameworks

Overview of cyber law: history, scope, and significance, Legal frameworks for cybersecurity:

international, national, and regional perspectives, legal principles and concepts in cyber law: jurisdiction, sovereignty, and attribution

Unit 2: Cybercrime Typologies and Legal Definitions

Classification of cybercrimes: hacking, malware, phishing, identity theft, etc.,Legal definitions of cybercrimes: statutes, regulations, and case law, Emerging trends and challenges in cybercrime enforcement

Unit 3: Legal Issues in Cyber Investigations and Evidence

Legal procedures for cyber investigations: search warrants, subpoenas, and surveillance, Collection and admissibility of digital evidence: chain of custody, authentication, and preservation, Legal challenges in prosecuting cyber offenders: jurisdictional issues, extradition, and cross-border cooperation

Unit 4: Cybersecurity Regulations and Compliance

Regulatory frameworks for cybersecurity: industry-specific regulations, privacy laws, and data protection regulations, Compliance requirements for organizations: cybersecurity standards, risk management frameworks, and compliance audits, Legal implications of data breaches: notification requirements, liability, and regulatory penalties

Unit 5: Legal and Ethical Issues in Cyber Defense and Incident Response

Legal aspects of cyber defense strategies: incident response planning, threat intelligence sharing, and cybersecurity incident reporting, Ethical considerations in cybersecurity: professional ethics, responsible disclosure, and ethical hacking, Legal challenges and best practices in cyber defense: liability, privacy concerns, and ethical dilemmas

Textbooks:

- "Cyber Law: Maximizing Safety and Minimizing Risk in Classrooms" by H. Jay Hickey
- "Cybercrime: Investigating High-Technology Computer Crime" by Robert Moore

Syllabus

DEPARTMENTAL ELECTIVE-1

CRYPTOGRAPHY & NETWORK SECURITY (CST-035)

L:T:P:: 3:0:0 **Credits-03**

COURSE OBJECTIVES: The objectives of the course are to

1. Explain the importance and application of each of confidentiality, integrity, authentication and availability.
2. Understand various cryptographic algorithms and basic categories of threats to computers and networks.
3. Describe the enhancements made to IPv4 by IPSec.
4. Understand Intrusions, intrusion detection, Web security and Firewalls.

COURSE OUTCOMES: On Successful completion of this course, the students will be able to

1. Identify the various attacks and its issues.
2. Learn usage of cryptographic algorithms for avoiding basic level threats.
3. Comprehend the issues involved in Integrity, Authentication and Key Management techniques.
4. Realize the importance of user authentication and Kerberos concepts.
5. Acquire the knowledge of network and system security domain.

Unit 1- Introduction of Cryptography: Introduction To security: Attacks, Services and Mechanisms, Conventional Encryption: Conventional Encryption Model, Steganography, Block Cipher Principles, DES Standard, DES Strength, Differential and Linear Cryptanalysis, Block Cipher Modes of Operations.Double DES, Triples DES, Blowfish, International Data Encryption Algorithm,Placement of Encryption Function, Key Distribution, Random Number Generation and Traffic confidentiality

Unit 2- Number Theory and Public Key Encryption: Fermat's and Euler's Theorem, Primality Testing, Chinese Remainder Theorem , Public-Key Cryptography: Principles of Public-Key Cryptosystems, RSA Algorithm.

Unit 3- Key Management: Key Management scenario in secret key and public key cryptography, Diffie Hellman Key Exchange algorithm, OAKLEY and ISAKMP key management protocol, Elliptic Curve Cryptography

Unit 4-Hash Functions: Message Authentication and Hash Functions: Authentication Requirements, Authentication Functions, Message Authentication Codes, Hash Function Birthday Attacks, Security of Hash Function and MACS, MD5 Message Digest Algorithm, Secure Hash Algorithm (SHA), Digital Signatures, Digital Signature Standard (DSS).

Unit 5- Network and System Security: Authentication Applications: Kerberos, X.509, Electronic Mail Security, Pretty Good Privacy (PGP),S/Mine Security: Architecture, Authentication Header, Encapsulating Security Payloads, Combining Security

Associations, Key Management, Web Security: Secure Socket Layer and Transport Layer Security, Secure Electronic Transaction (SET), System Security: Intruders, Viruses, Firewall Design Principles, Trusted Systems.

TEXT BOOKS:

1. Cryptography and Network Security - Principles and Practice: William Stallings, Pearson Education, 6th Edition.
2. Cryptography and Network Security: Atul Kahate, Mc Graw Hill, 3rd Edition.

REFERENCE BOOKS:

1. Cryptography and Network Security: C K Shyamala, N Harini, Dr T R Padmanabhan, Wiley India, 1st Edition.
2. Cryptography and Network Security: Forouzan Mukhopadhyay, Mc Graw Hill, 3rd Edition.
3. Information Security, Principles, and Practice: Mark Stamp, Wiley India.
4. Principles of Computer Security: WM. Arthur Conklin, Greg White, TMH.
5. Introduction to Network Security: Neal Krawetz, CENGAGE Learning.
6. Network Security and Cryptography: Bernard Menezes, CENGAGE Learning

Syllabus

ETHICAL HACKING AND PENETRATION TESTING LAB (CYP-105)

L:T:P:0:0:2 **CREDITS:01**

LIST OF EXPERIMENTS

1 Footprinting and Reconnaissance:Performing footprinting using Google Hacking, website information, information about an archived website, to extract contents of a website, to trace any received email, to fetch DNS information.

2 Scanning networks, Enumeration and sniffing: Use port scanning. network scanning tools, IDS tool, sniffing tool and generate reports.

3 Malware Threats: Worms, viruses,Trojans:Use Password cracking, Dictionary attack.,Encrypt and decrypt passwords, DoS attack,ARP poisoning in windows, Ifconfig, ping,netstat, traceroute, Steganography tools.Self-Learning Topics: using additionalhacking tools.

4 Developing and implementing malwares :Creating a simple keylogger in python, creating a virus, creating a trojan. Self-Learning Topics: Additional implementation of hacking tools.

5 Hacking web servers, web applications:Hacking a website by Remote File Inclusion,Disguise as Google Bot to view hidden content of a website, to use Kaspersky for Lifetime without Patch

6 sql injection and Session hijacking : SQL injection for website hacking, session hijacking. Self Learning Topics: using additional of hacking tools.

7 Wireless network hacking, cloud computing security, cryptography : Using Cryptool to encrypt and decrypt password, implement encryption and decryption using Ceaser Cipher. Self-Learning Topics: implementing additional encryption algorithms.
8 Pen testing : Penetration Testing using Metasploit and metasploitable,

Syllabus

AI AND ML LAB (CYP-106)

L:T:P:0:0:2 **CREDITS:01**

Artificial Intelligence Programs Using PROLOG

1. Study of PROLOG Programming language and its Functions. Write simple facts for the statements using PROLOG.

2. Implementation of Depth First Search for Water Jug problem.

3. Implementation of Breadth First Search for Tic-Tac-Toe problem.

4. Solve 8-puzzle problem using Best First Search. Write a program to Implement A*.

5. Write a PROLOG program to solve N-Queens problem.

6. Implementation of Traveling Salesman Problem.

Machine Learning Programs Using Python

1. Implementation of Python Basic Libraries such as Statistics, Math, Numpy and Scipy

a) Usage of methods such as floor(), ceil(), sqrt(), isqrt(), gcd() etc.

b) Usage of attributes of array such as ndim, shape, size, methods such as sum(), mean(), sort(), sin() etc.

c) Usage of methods such as det(), eig() etc.

d) Consider a list datatype (1D) then reshape it into 2D, 3D matrix using numpy

e) Generate random matrices using numpy

f) Find the determinant of a matrix using scipy

g) Find eigenvalue and eigenvector of a matrix using scipy

2. Implementation of Python Libraries for ML application such as Pandas andMatplotlib.

a) Create a Series using pandas and display

b) Access the index and the values of our Series

c) Compare an array using Numpy with a series using pandas

d) Define Series objects with individual indices

e) Access single value of a series

f) Load datasets in a Dataframe variable using pandas

g) Usage of different methods in Matplotlib.

3. a) Creation and Loading different types of datasets in Python using the required libraries.

i. Creation using pandas

ii. Loading CSV dataset files using Pandas

iii. Loading datasets using sklearn

b) Write a python program to compute Mean, Median, Mode, Variance, Standard Deviation using Datasets

c) Demonstrate various data pre-processing techniques for a given dataset.

Write a python program to compute

i. Reshaping the data,

ii. Filtering the data,

iii. Merging the data

iv. Handling the missing values in datasets

v. Feature Normalization: Min-max normalization

4. a) Write a program to demonstrate the working of the decision tree based ID3 algorithm by considering a dataset.

b) Consider a dataset, use Random Forest to predict the output class. Vary the number of trees as follows and compare the results: i. 20 ii. 50 iii. 100 iv. 200 v. 500

5. a) Write a Python program to implement Simple Linear Regression and plot the graph. b) Implementation of Logistic Regression for iris using sklearn.

6. a) Build KNN Classification model for a given dataset. Vary the number of k values as follows and compare the results: i. 1 ii. 3 iii. 5 iv. 7 v. 11

b) Implement Support Vector Machine for a dataset and compare the accuracy by applying the following kernel functions: i. Linear ii. Polynomial iii. RBF

c) Write a python program to implement K-Means clustering Algorithm. Vary the number of k values as follows and compare the results: i. 1 ii. 3 iii. 5 iv. 7

Syllabus

DIGITAL FORENSIC LAB (CYP-107)

L:T:P:0:0:2 **CREDITS:01**

LIST EXPERIMENTS

1.Study of Computer Forensics and different tools used for forensic investigation

2 Live Forensics Case Investigation using Autopsy

How to Recover Deleted Files using Forensics Tools

4 Find Last Connected USB on your system (USB Forensics)

5 How to View Last Activity of Your PC

6 How to Extracting Browser Artifacts

7 Comparison of two Files for forensics investigation by Compare IT software

8 How to Collect Email Evidence in Victim PC

9 Study the steps for hiding and extract any text file behind an image file/ Audio file using Command Prompt.

10 How to Extract Exchangeable image file format (EXIF) Data from Image Files using Exifreader Software

Syllabus

DESIGN PROJECT (CYP-108)

L:T:P:: 0:0:4 **Credits-02**

COURSE OBJECTIVES: The objectives of the course are to

1. Develop skills in doing literature survey, technical presentation, and report preparation.
2. Enable project identification and execution of preliminary works on final semester project.

COURSE OUTCOMES: On successful completion of this course, the students shall be able to

1. Discover potential research areas in the field of information technology.
2. Create very precise specifications of the IT solution to be designed.
3. Have introduction to the vast array of literature available about the various research challenges in the field of IT.
4. Use all concepts of IT in creating a solution for a problem.
5. Have a glimpse of real world problems and challenges that need IT-based solutions.

Syllabus

ESSENCE OF INDIAN TRADITIONAL KNOWLEDGE (AHT-010)

L:T:P:: 2:0:0 **Credits-0**

COURSE OBJECTIVES: The objectives of this course are to

1. To facilitate the students with the concepts of Indian traditional knowledge and to make them understand the Importance of roots of knowledge system.
2. To make the students understand the traditional knowledge and analyses it and apply it to their day to day life.
3. To make the students know the need and importance of protecting traditional knowledge.
4. To make the students understand the concepts of Intellectual property to protect the traditional knowledge.
5. This course is also concentrating on various acts in protecting the environment and Knowledge management impact on various sectors in the economy development of the country.

COURSE OUTCOMES:

On successful completion of the course, the students will be able to

1. Understand the concept of Traditional knowledge and its importance.
2. Know the need and importance of protecting traditional knowledge.
3. Know the various enactments related to the protection of traditional knowledge.
4. Understand the concepts of Intellectual property to protect the traditional knowledge.
5. Know the contribution of scientists of different areas.

Unit – 1 Introduction to Traditional and Culture Knowledge

Define culture, traditional, civilization and heritage knowledge, nature and characteristics, scope and importance, kinds of traditional knowledge, the physical and social contexts in which traditional knowledge develop, the historical impact of social change on traditional knowledge systems. Indigenous Knowledge (IK). Indigenous traditional knowledge Vs western traditional knowledge vis-à-vis formal knowledge.

Unit-2 Protection of Traditional Knowledge

Protection of traditional knowledge: The need for protecting traditional knowledge Significance of traditional knowledge Protection, value of traditional knowledge in global economy, Role of Government to harness traditional knowledge.

Unit – 3 Traditional Knowledge and Intellectual Property

Systems of traditional knowledge protection, Legal concepts for the protection of traditional knowledge, Certain non IPR mechanisms of traditional knowledge protection, Patents and traditional knowledge, Strategies to increase protection of traditional knowledge, Global legal forums for increasing protection of Indian Traditional Knowledge.

Unit – 4 Traditional Knowledge in Different Sectors

Traditional knowledge in engineering, biotechnology and agriculture, traditional medicine system, Traditional societies depend on it for their food and healthcare needs, Importance of conservation and sustainable development of environment, Management of biodiversity, Food security of the country and protection of traditional knowledge.

Unit – 5 Education System in India

Syllabus

Education in ancient, medieval and modern India, aims of education, subjects, languages, Science and Scientists of Ancient India, Scientists of Medieval India, Scientists of Modern India. The role Gurukulas in Education System, Value based Education.

Text/Reference Books:

1. Traditional Knowledge System in India by Amit Jha Atlantic publishers, 2002.
2. "Knowledge Traditions and Practices of India" Kapil Kapoor1, Michel Danino2.
3. Traditional Knowledge System in India, by Amit Jha, 2009.
4. Satya Prakash, “Founders of Sciences in Ancient India”, Vijay Kumar Publisher, 1989
5. Traditional Knowledge System and Technology in India by Basanta Kumar Mohanta and Vipin Kumar Singh Pratibha Prakashan 2012.

Syllabus

VEER MADHO SINGH BHANDARI UTTARAKHAND TECHNICAL UNIVERSITY

(Formerly Uttarakhand Technical University, Dehradun Established by Uttarakhand State Govt. wide Act no. 415 of 2005)
Suddhowala, PO-Chandanwadi, Premnagar, Dehradun, Uttarakhand (Website- www.uktech.ac.in)

SYLLABUS

For

B. TECH

Cyber Security

4th Year

Effective From – Session 2025-26

Syllabus

SEMESTER-VII													
S. NO.	Subject Codes	Category	Subject	Periods			Evaluation Scheme					Subject Total	Credit
							Sessional Exam			ESE			
				L	T	P	CT	TA	Total	TE	PE		
1	AHT-015	HSC	Rural Development Administration and Planning	3	1	0	30	20	50	100		150	3
2	CYT-115	DC	Reverse Engineering Malware: Malware Analysis tools and Techniques	3	1	0	30	20	50	100		150	4
3	CST-043	DC	Big Data analytics	3	1	0	30	20	50	100		150	4
4		DE	Departmental Elective-2	3	0	0	30	20	50	100		150	3
5	CYT-120	DC	Open-Source Intelligence	3	0	0	30	20	50	100		150	3
6	CYT-121	DC	Cloud Security	3	1	0	30	20	50	100		150	4
7	CYP-109	DLC	Reverse Engineering Malware: Malware Analysis tools and Techniques Lab	0	0	2		25	25		25	50	1
8	CYP-110	DLC	Cloud Security Lab	0	0	2			50			50	1
9	CYP-111	DLC	Open-Source Intelligence Lab	0	0	2		25	25		25	50	1
10	CYP-112	DLC	Design Project	0	0	4		25	25		25	50	2
11	CYP-113	DLC	Mini Project-III or Internship-III*	0	0	2			50			50	2
12	GP-007	NC	General Proficiency						50			50	
13			Total	18	2	12						1200	27
	*The Internship-III (4-6weeks) will be conducted during summer break after the VI semester and will be assessed during VII semester.												

Departmental Elective-2		
S. No.	**Subject Code**	**Subject Name**
1	CYT-116	Threat Intelligence
2	CYT-117	Intrusion Detection System
3	CYT-118	Cyber Security & AI
4	DST-103	Web & Social Media Analytics
5	CYT-119	Secure Software Design & Enterprise Computing

Abbreviations: L-No. of Lecture hours per week, **T**-No. of Tutorial hours per week, **P**-No. of Practical hours per week, **CT**-Class Test Marks, **TA**-Marks of teacher's assessment including student's class performance and attendance, **PS**-Practical Sessional Marks, **ESE**-End Semester Examination, **TE**- Theory Examination Marks, PE- Practical External Examination Marks

1 Hr Lecture	1 Hr Tutorial	2 or 3 Hr Practical
1 Credit	**1 Credit**	**1 Credit**

Syllabus

SEMESTER-VIII													
S. NO.	**Subject Codes**	**Category**	**Subject**	**Periods**			**Evaluation Scheme**					**Subject Total**	**Credit**
							Sessional Exam			**ESE**			
				L	T	P	CT	TA	Total	TE	PE		
1	CYP-114	DLC	*Project Based Internship in Industry				200	100	300	250	500	1050	20
6	GP-008	NC	General Proficiency						50			50	
			Total									1100	20

*For Project Based Internship in Industry the Student will be mentored by two mentors:

1. The first mentor will be assigned by the institute
2. The second mentor will be assigned by the industry

For evaluation of the Project:

1. For evaluating sessional exam:
   - i) The mentor from industry will conduct two Class Test(CT) of 50 marks each and will do Teacher Assessment (TA) of 50 marks, constituting of total 150 marks.
   - ii) The mentor from institute will conduct two Class Test(CT) of 50 marks each and will do Teacher Assessment (TA) of 50 marks, constituting of total 150 marks.
   - iii) Therefore, the total of sessional exam will be 300.
2. For evaluating End Semester Exam (ESE)
   - i) For evaluation of the Project, a panel will be constituted by the University comprising a representative from university, the mentor from institute, the mentor from industry, Dean/Head of the Department concerned.
   - ii) The evaluation will be based on:
     a. Theory exam (TE) will comprise of Report of the Project of 250 marks.
     b. Practical exam (PE) will comprise of: PowerPoint Presentation of 200 marks and Viva-Voce of 300 marks, making it total of 500 marks.
3. Industrial internships, for which some of the topics are listed below
   a) Web Attack and Defence
   b) Network Attack and Defence
   c) Data Center Security
   d) Social media Security and OS Int
   e) Mobile and App Security
   f) IoT/OT Security
   g) SoC /SIEM operations etc

Abbreviations: L-No. of Lecture hours per week, **T**-No. of Tutorial hours per week, **P**-No. of Practical hours per week, **CT**-Class Test Marks, **TA**-Marks of teacher's assessment including student's class performance and attendance, **PS**-Practical Sessional Marks, **ESE**-End Semester Examination, **TE**- Theory Examination Marks, PE- Practical External Examination Marks

1 Hr Lecture	**1 Hr Tutorial**	**2 or 3 Hr Practical**
1 Credit	**1 Credit**	**1 Credit**

Syllabus

RURAL DEVELOPMENT: ADMINISTRATION AND PLANNING (AHT-015)

L:T:P:: 3:1:0 **Credits-03**

Course Objectives

This course enables the students to:

1. Gain knowledge on the concepts related to administration, its importance and various approaches of Development Administration.
2. Gain skills on New Public Management, Public Grievances and Redressal Mechanisms, Accountability and Transparency in Administration and e-governance in the rural development sector.
3. Develop their competency on the role of Bureaucracy in Rural Development.

Course Outcomes

After completion of the course student will be able to:

1. Students can understand the definitions, concepts and components of Rural Development.
2. Students will know the importance, structure, significance, resources of Indian rural economy.
3. Students will have a clear idea about the area development programmes and its impact.
4. Students will be able to acquire knowledge about rural entrepreneurship.
5. Students will be able to understand about the using of different methods for human resource planning.

Course Contents

UNIT-I: **(8 hours)**

Rural Planning & Development: Concepts of Rural Development, Basic elements of rural Development, and Importance of Rural Development for creation of Sustainable Livelihoods, An overview of Policies and Programmes for Rural Development- Programmes in the agricultural sector, Programmes in the Social Security, Programmes in area of Social Sector.

UNIT-II: **(8 hours)**

Rural Development Programmes: Sriniketan experiment, Gurgaon experiment, Marthandam experiment, Baroda experiment, Firkha development scheme, Etawapilot project, Nilokheri experiment, approaches to rural community development: Tagore, Gandhi etc.

UNIT-III: **(8 hours)**

Panchayati Raj & Rural Administration: Administrative Structure: bureaucracy, structure of administration; Panchayati Raj Institutions Emergence and Growth of Panchayati Raj Institutions in India; People and Panchayati Raj; Financial Organizations in Panchayati Raj Institutions, Structure of rural finance, Government & Non-Government Organizations / Community Based Organizations, Concept of Self help group.

UNIT-IV: **(8 hours)**

Human Resource Development in Rural Sector: Need for Human Resource Development, Elements of Human Resource Development in Rural Sector Dimensions of HRD for rural development-Health,

Syllabus

Education, Energy, Skill Development, Training, Nutritional Status access to basic amenities – Population composition.

UNIT-V: **(8 hours)**

Rural Industrialization and Entrepreneurship: Concept of Rural Industrialization, Gandhian approach to Rural Industrialization, Appropriate Technology for Rural Industries, Entrepreneurship and Rural Industrialization- Problems and diagnosis of Rural Entrepreneurship in India, with special reference to Women Entrepreneurship; Development of Small Entrepreneurs in India, need for and scope of entrepreneurship in Rural area.

Text Books/References:

1. Corporate Social Responsibility: An Ethical Approach - Mark S. Schwartz.
2. Katar Singh: Rural Development in India – Theory History and Policy.
3. Todaro M.P. Economic Development in III World war.
4. Arora R.C – Integrated Rural Development in India.
5. Dhandekar V.M and Rath N poverty in India.
6. A.N.Agarwal and Kundana Lal: Rural Economy of India
7. B.K.Prasad: Rural Development-Sarup& Son's Publications.

Syllabus

Reverse Engineering Malware: Malware Analysis Tools and Techniques (CYT-116)

L:T:P:: 3:1:0 **Credits-04**

Course Objectives:

- Understand the fundamental concepts of malware analysis and reverse engineering.
- Learn various malware analysis tools and techniques used in the process of reverse engineering.
- Develop practical skills in analyzing malware samples to identify their behavior, capabilities, and intent.
- Explore advanced topics in malware analysis, such as code obfuscation, anti-analysis techniques, and malware evasion tactics.

Course Outcomes:

- Students will gain a comprehensive understanding of malware analysis methodologies, including static analysis, dynamic analysis, and behavioral analysis.
- Students will become proficient in using a variety of malware analysis tools, such as disassemblers, debuggers, sandboxes, and network traffic analyzers.
- Students will be able to analyze real-world malware samples to extract indicators of compromise (IOCs), understand their functionality, and assess their potential impact.
- Students will develop the skills to reverse engineer malware to uncover vulnerabilities, develop signatures for detection, and devise strategies for mitigation and remediation.

Course Description:

This course provides an in-depth exploration of malware analysis techniques, focusing on reverse engineering methods to dissect and understand malicious software. Students will learn how to use various tools and techniques to analyze malware samples, including static and dynamic analysis, code disassembly, and behavior monitoring.

Prerequisites:

Basic understanding of computer architecture, operating systems, and programming concepts.

Unit 1: Introduction to Malware Analysis

Overview of malware types and classification,Importance of malware analysis in cybersecurity, Legal and ethical considerations in malware research

Unit 2: Static Malware Analysis Techniques

Introduction to static analysis: file identification, metadata extraction, and hash analysis, PE file format

analysis using tools like PEiD and PEview, Identifying malware signatures and patterns using antivirus engines and YARA rules

Unit 3: Dynamic Malware Analysis Techniques

Introduction to dynamic analysis: sandboxing, virtualization, and runtime monitoring, Setting up a malware analysis environment: Cuckoo Sandbox, REMnux, and other tools,Analyzing malware behavior using tools like Process Monitor, Wireshark, and Regshot

Unit 4: Code Disassembly and Reverse Engineering

Introduction to code disassembly: disassemblers, decompilers, and debugger tools, Analyzing malware code using IDA Pro and Ghidra, Reverse engineering malware binaries to understand functionality and behavior

Unit 5: Malware Obfuscation and Anti-Analysis Techniques

Understanding malware obfuscation techniques: packing, encryption, and code manipulation,Techniques for bypassing anti-analysis mechanisms: debugger detection, environment checks, and anti-VM tricks, Countermeasures and best practices for overcoming malware obfuscation and anti-analysis challenges

Textbooks:

- "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" by Michael Sikorski and Andrew Honig
- "The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler" by Chris Eagle

Syllabus

BIG DATA ANALYTICS (CST-043)

L:T:P:: 3:1:0 **Credits-04**

COURSE OBJECTIVES: The objectives of the course are to

1. Make students comfortable with tools and techniques required in handling large amounts of datasets.
2. Uncover various terminologies and techniques used in Big Data.
3. Use several tools publicly available to illustrate the application of these techniques.
4. Know about the research that requires the integration of large amounts of data.

COURSE OUTCOMES: On successful completion of this course, the students will be able to

1. Identify and distinguish big data analytics applications.
2. Design efficient algorithms for mining the data from large volumes.
3. Analyze the HADOOP and Map Reduce technologies associated with big data analytics.
4. Understand the fundamentals of various big data analytics techniques.
5. Present cases involving big data analytics in solving practical problems.

UNIT – I

Introduction to big data: Introduction to Big Data Platform – Challenges of Conventional Systems - Intelligent data analysis – Nature of Data - Analytic Processes and Tools - Analysis vs Reporting.

UNIT – II

Mining data streams: Introduction to Streams Concepts – Stream Data Model and Architecture - Stream Computing - Sampling Data in a Stream – Filtering Streams –Counting Distinct Elements in a Stream – Estimating Moments – Counting Oneness ina Window – Decaying Window - Real time Analytics Platform(RTAP) Applications – Case Studies - Real Time Sentiment Analysis- Stock Market Predictions.

UNIT – III

Hadoop: History of Hadoop- the Hadoop Distributed File System – Components of Hadoop Analyzing the Data with Hadoop- Scaling Out- Hadoop Streaming- Design of HDFS-Java interfaces to HDFS Basics- Developing a Map Reduce Application- How Map Reduce Works-Anatomy of a Map Reduce Job Run-Failures-Job Scheduling-Shuffle and Sort – Task execution - Map Reduce Types and Formats- Map Reduce Features-Hadoop environment.

UNIT – IV

Frameworks: Applications on Big Data Using Pig and Hive – Data processing operatorsin Pig – Hive services – HiveQL – Querying Data in Hive - fundamentals of HBase and Zookeeper - IBM Infosphere Big Insights and Streams.

UNIT – V

Predictive Analytics- Simple linear regression- Multiple linear regression- Interpretation of regression coefficients. Visualizations - Visual data analysis techniques- interaction techniques - Systems and applications.

TEXTBOOKS:

1. Michael Berthold, David J. Hand, "Intelligent Data Analysis", Springer, 2007.
2. Tom White "Hadoop: The Definitive Guide" Third Edition, O'reilly Media, 2012.
3. Chris Eaton, Dirk DeRoos, Tom Deutsch, George Lapis, Paul Zikopoulos, "Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data", McGrawHill Publishing, 2012.
4. Anand Rajaraman and Jeffrey David Ullman, "Mining of Massive Datasets", CUP, 2012.
5. Bill Franks, "Taming the Big Data Tidal Wave: Finding Opportunities in Huge Data Streams with Advanced Analytics", John Wiley& sons, 2012.

REFERENCE BOOKS:

1. Michael Minelli, Michele Chambers, and Ambiga Dhiraj, Big Data, Big Analytics: Emerging Business Intelligence and Analytic Trends for Today's Businesses, Wiley,2013.
2. Frank J. Ohlhorst, Big Data Analytics: Turning Big Data into Big Money, Wiley, 2012.
3. Arvind Sathi, Big Data Analytics: Disruptive Technologies for Changing the Game, MC Press, 2012.
4. Glenn J. Myatt, "Making Sense of Data", John Wiley & Sons, 2007.
5. Pete Warden, "Big Data Glossary", O'Reilly, 2011.
6. Jeffrey Aven, Hadoop in 24 hours, person education 2018.
7. Jiawei Han, Micheline Kamber "Data Mining Concepts and Techniques", 2nd Edition, Elsevier, Reprinted 2008.
8. Da Ruan, Guoquing Chen, Etienne E.Kerre, Geert Wets, "Intelligent Data Mining", Springer, 2007.
9. Paul Zikopoulos, Dirkde Roos, Krishnan Parasuraman, Thomas Deutsch, James Giles , David Corrigan, "Harness the Power of Big Data The IBM Big Data Platform", Tata McGraw Hill Publications, 2012.
10. Arshdeep Bahga, Vijay Madisetti, "Big Data Science & Analytics: A Hands- On Approach ",VPT, 2016
11. Bart Baesens "Analytics in a Big Data World: The Essential Guide to Data Science and its Applications (WILEY Big Data Series)", John Wiley & Sons,2014.

Syllabus

Departmental Elective -2

Threat Intelligence (CYT-117)

L:T:P:3:0:0 **CREDIT:03**

Course objectives:
1. Introduce the concepts of threat intelligence and its life cycle.
2. Learn threat intelligence for security operations and incident response.
3. Know about how to Identify and create intelligence requirements through practices such as threat modeling.
4. Understand and develop skills in tactical, operational, and strategic-level threat intelligence.
5. Generate threat intelligence to detect, respond to, and defeat focused and targeted threats.

Course Outcomes:
1: Define the basic concepts, terminology and Threat Intelligence life cycle.
2: Discuss various applications and characteristics of Threat Intelligence.
3: Examine Vulnerabilities, Risks, and Mitigation strategies.
4: Explore fraud prevention systems and risk models.
5: Review third-party risk and various forms of digital risks.

UNIT 1:

Introduction to Threat Intelligence?: What Have You Heard About Threat Intelligence?, Why Is Threat Intelligence Important?, Who Can Benefit From Threat Intelligence?, Data and Information Are Not Intelligence, Two Types of Threat Intelligence, Operational Threat Intelligence, Strategic Threat Intelligence, The Role of Threat Data, Feeds, The Role of Private Channels and the Dark Web; The Threat Intelligence Lifecycle: The Six Phases of the Threat Intelligence Lifecycle, Direction, Collection, Processing, Analysis, Dissemination, Feedback, Tools and People.

UNIT 2:

Threat Intelligence for Security Operations: Responsibilities of the SOC Team, The Overwhelming Volume of Alerts, Context Is King: Triage requires lots of context, Use case: Correlating and enriching alerts, Improving the "Time to No", Beyond Triage; Threat Intelligence for Incident Response: Continuing Challenges; A skills gap; Too many alerts; too little time; Time to response is rising; A piecemeal approach; The Reactivity Problem; Minimizing Reactivity in Incident Response: Identification of probable threats, Prioritization; Strengthening Incident Response With Threat Intelligence; Threat Intelligence in Action: Use case: Prepare processes in advance, Use case: Scope and contain incidents; Essential Characteristics of Threat Intelligence: for Incident Response, Comprehensive, Relevant, Contextualized, Integrated.

UNIT 3:

Threat Intelligence for Vulnerability Management: The Vulnerability Problem by the Numbers: Zero day does not mean top priority, Time is of the essence; Assess Risk Based on Exploitability: Severity ratings can be misleading; The Genesis of Threat Intelligence: Vulnerability Databases: Exploitability versus exploitation, Next week versus now; Threat Intelligence and Real Risk: Internal vulnerability scanning, Risk milestones for vulnerabilities, Understanding the adversary; Sources of Intelligence; Use Case: Cross-Referencing Intelligence; Bridging the Risk Gaps Between Security, Operations, and Business Leadership. Threat Intelligence for Security Leaders: Risk Management: Internal data is not enough, Sharpening the focus; Mitigation: People, Processes, and Tools: Early warnings; Investment; Communication; Supporting Security Leaders; The Security Skills Gap; Intelligence to Manage Better.

UNIT 4:

Threat Intelligence for Risk Analysis: The FAIR Risk Model: Measurements and transparency are key; Threat Intelligence and Threat Probabilities; Threat Intelligence and the Cost of Attacks; Threat Intelligence for Fraud Prevention: Stand and Deliver; Know Your Enemy; Criminal Communities and the Dark Web: Gated communities, A strength — and a weakness; Connecting the Dots for Fraud Prevention: Use case: Payment fraud, Use case: Compromised data, Use case: Typosquatting and fraudulent domains.

UNIT 5:

Syllabus

Third-Party Risk Looms Large; Traditional Risk Assessments Fall Short; Three Things to Look for in Threat Intelligence: Automation and machine learning, Real-time updates to risk scores, Transparent risk assessments; Responding to High Third-Party Risk Scores; Threat Intelligence for Digital Risk Protection: Being Online Is Being at Risk; Types of Digital Risk; Uncovering Evidence of Breaches on the Web; Uncovering Evidence of Brand Impersonation and Abuse; Critical Qualities for Threat Intelligence Solutions.

Text Books(s)

1. Zane Pokorny, The Threat Intelligence Handbook: Moving Toward a Security Intelligence Program", 2nd Edition, CyberEdge Group, 2019

Coursera Courses: 1. https://www.coursera.org/learn/ibm-cyber-threat-intelligence

Reference Book(s)

1. Ali Dehghantanha, Mauro Conti, Tooska Dargahi, Cyber Threat Intelligence, Springer, 2018.

2. The Threat Intelligence Handbook: A Practical Guide for Security Teams to Unlocking the Power of Intelligence, CyberEdge Group, 2018.

3. www.cyber-edge.com

Syllabus

Departmental Elective -2

Intrusion Detection System (CYT-118)

L:T:P:3:0:0 **CREDIT:03**

COURSE OBJECTIVES:

1. To introduce basic concepts of intrusion detection system.
2. To understand Intrusion Prevention Systems, Network IDs protocol and model for intrusion analysis.
3. To Understand when, where, how, and why to apply Intrusion Detection tools and techniques in order to improve the security posture of an enterprise.
4. To Apply knowledge of the fundamentals and history of Intrusion Detection in order to avoid common pitfalls in the creation and evaluation of new Intrusion Detection Systems.
5. To learn agent development for intrusion detection and architectural models of IDs and IPs.

COURSE OUTCOMES:

1. Students will be introduced to basic concepts of intrusion detection system.
2. Students will be able to understand Intrusion Prevention Systems, Network IDs protocol and model for intrusion analysis.
3. Students will be able to understand when, where, how, and why to apply Intrusion Detection tools and techniques in order to improve the security posture of an enterprise.
4. Students will be able to apply knowledge of the fundamentals and history of Intrusion Detection in order to avoid common pitfalls in the creation and evaluation of new Intrusion Detection Systems.
5. Students will be able to learn agent development for intrusion detection and architectural models of IDs and IPs

UNIT-I:

History of Intrusion detection, Audit, Concept and definition , Internal and external threats to data, attacks, Need and types of IDS, Information sources Host based information sources, Network based information sources.

UNIT-II:

Intrusion Prevention Systems, Network IDs protocol based IDs ,Hybrid IDs, Analysis schemes, thinking about intrusion. A model for intrusion analysis , techniques Responses requirement of responses, types of responses mapping responses to policy Vulnerability analysis, credential analysis non credential analysis.

UNIT-III:

Introduction to Snort, Snort Installation Scenarios, Installing Snort, Running Snort on Multiple Network Interfaces, Snort Command Line Options. Step-By-Step Procedure to Compile and Install Snort Location of Snort Files, Snort Modes Snort Alert Modes

UNIT-IV:

Working with Snort Rules, Rule Headers, Rule Options, The Snort Configuration File etc. Plugins, Preprocessors and Output Modules, Using Snort with MySQL

Syllabus

UNIT-V:

Using ACID and Snort Snarf with Snort, Agent development for intrusion detection, Architecture models of IDs and IPs.

TEXT BOOKS:

1. Rafeeq Rehman : " Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID," 1st Edition, Prentice Hall , 2003.

REFERENCES:

1. Christopher Kruegel,Fredrik Valeur, Giovanni Vigna: "Intrusion Detection and Correlation Challenges and Solutions", 1st Edition, Springer, 2005.
2. Carl Endorf, Eugene Schultz and Jim Mellander " Intrusion Detection & Prevention", 1st Edition, Tata McGraw-Hill, 2004.
3. Stephen Northcutt, Judy Novak : "Network Intrusion Detection", 3rd Edition, New Riders Publishing, 2002.
4. T. Fahringer, R. Prodan, "A Text book on Grid Application Development and Computing Environment". 6th Edition, KhannaPublihsers, 2012

Syllabus

Departmental Elective -2

CYBER SECURITY AND AI (CYT-119)

L:T:P:: 3:0:0 **Credits-03**

Course objectives:

1. To familiarize various types of cyber-attacks and cyber-crimes
2. To give an overview of the cyber laws
3. To study the defensive techniques against these attacks
4. To train the students to understand different types of AI agents, various AI search algorithms
5. fundamentals of knowledge representation

UNIT - I

Introduction to Cyber Security: Basic Cyber Security Concepts, layers of security, Vulnerability, threat, Harmful acts, Internet Governance – Challenges and Constraints, Computer Criminals, CIA Triad, Assets and Threat, motive of attackers, active attacks, passive attacks, Software attacks, hardware attacks, Spectrum of attacks, Taxonomy of various attacks, IP spoofing, Methods of defense, Security Models, risk management, Cyber Threats-Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage, etc., Comprehensive Cyber Security Policy.

UNIT - II

Cyberspace and the Law & Cyber Forensics: Introduction, Cyber Security Regulations, Roles of International Law. The INDIAN Cyberspace, National Cyber Security Policy. Introduction, Historical background of Cyber forensics, Digital Forensics Science, The Need for Computer Forensics, Cyber Forensics and Digital evidence, Forensics Analysis of Email, Digital Forensics Lifecycle, Forensics Investigation, Challenges in Computer Forensics, Special Techniques for Forensics Auditing.

UNIT - III

Cybercrime: Mobile and Wireless Devices: Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for Organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era, Laptops.

UNIT- IV

Cyber Security: Organizational Implications: Introduction, cost of cybercrimes and IPR issues, web threats for organizations, security and privacy implications, social media marketing: security risks and perils for organizations, social computing and the associated challenges for organizations. Cybercrime and Cyber terrorism: Introduction, intellectual property in the cyberspace, the ethical dimension of cybercrimes the psychology, mindset and skills of hackers and other cyber criminals.

UNIT- V

Syllabus

Introduction: AI problems, Agents and Environments, Structure of Agents, Problem Solving Agents Basic Search Strategies: Problem Spaces, Uninformed Search (Breadth-First, Depth-First Search, Depth-first with Iterative Deepening), Heuristic Search (Hill Climbing, Generic Best-First, A*), Constraint Satisfaction (Backtracking, Local Search)

UNIT -VI

Advanced Search: Constructing Search Trees, Stochastic Search, A* Search Implementation, Minimax Search, Alpha-Beta Pruning Basic Knowledge Representation and Reasoning: Propositional Logic, First-Order Logic, Forward Chaining and Backward Chaining, Introduction to Probabilistic Reasoning, Bayes Theorem

TEXT BOOKS:

1. Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley

2. B. B. Gupta, D. P. Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335, 2018.

3. Russell, S. and Norvig, P, Artificial Intelligence: A Modern Approach, Third Edition, PrenticeHall, 2010.

REFERENCE BOOK:

1. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press.

2. Introduction to Cyber Security, Chwan-Hwa(john) Wu,J. David Irwin, CRC Press T&F Group.

3. Artificial Intelligence, Elaine Rich, Kevin Knight, Shivasankar B. Nair, The McGraw Hill publications, Third Edition, 2009.

4. George F. Luger, Artificial Intelligence: Structures and Strategies for Complex Problem Solving, Pearson Education, 6th ed., 2009.

Syllabus

DEPARTMENTAL ELECTIVE-2

WEB AND SOCIAL MEDIA ANALYTICS (DST-103)

L:T:P:: 3:0:0 **Credits-03**

Course Objectives: Exposure to various web and social media analytic techniques.
1. Understand the role of web analytics within the digital marketing landscape.
2. To study methods to transform social media data into marketing insights.
3. Understand how to effectively use insights to support website design decisions, campaign optimization, search analytics, etc.

Course Outcomes:
1. Knowledge on decision support systems.
2. Apply natural language processing concepts on text analytics.
3. Understand sentiment analysis.
4. Knowledge on search engine optimization and web analytics.
5.

UNIT - I

An Overview of Business Intelligence, Analytics, and Decision Support: Analytics to Manage a Vaccine Supply Chain Effectively and Safely, Changing Business Environments and Computerized Decision Support, Information Systems Support for Decision Making, The Concept of Decision Support Systems (DSS), Business Analytics Overview, Brief Introduction to Big Data Analytics.

UNIT - II

Text Analytics and Text Mining: Machine Versus Men on Jeopardy!: The Story of Watson, Text Analytics and Text Mining Concepts and Definitions, Natural Language Processing, Text Mining Applications, Text Mining Process, Text Mining Tools.

UNIT - III

Sentiment Analysis: Sentiment Analysis Overview, Sentiment Analysis Applications, Sentiment Analysis Process, Sentiment Analysis and Speech Analytics.

UNIT - IV

Web Analytics, Web Mining: Security First Insurance Deepens Connection with Policyholders, Web Mining Overview, Web Content and Web Structure Mining, Search Engines, Search Engine Optimization, Web Usage Mining (Web Analytics), Web Analytics Maturity Model and Web Analytics Tools.

UNIT - V

Social Analytics and Social Network Analysis: Social Analytics and Social Network Analysis, Social Media Definitions and Concepts, Social Media Analytics.

Prescriptive Analytics - Optimization and Multi-Criteria Systems: Multiple Goals, Sensitivity Analysis, What-If Analysis, and Goal Seeking.

Syllabus

TEXT BOOK:

1. Ramesh Sharda, Dursun Delen, Efraim Turban, BUSINESS INTELLIGENCE AND ANALYTICS: SYSTEMS FOR DECISION SUPPORT, Pearson Education.

REFERENCE BOOKS:

1. Rajiv Sabherwal, Irma Becerra-Fernandez," Business Intelligence – Practice, Technologies and Management", John Wiley 2011.
2. Lariss T. Moss, ShakuAtre, "Business Intelligence Roadmap", Addison-Wesley It Service.
3. Yuli Vasiliev, "Oracle Business Intelligence: The Condensed Guide to Analysis and Reporting", SPD Shroff, 2012.

Syllabus

Departmental Elective-2

SECURE SOFTWARE DESIGN AND ENTERPRISE COMPUTING (CYT-119)

L:T:P:3:0:0 **CREDIT:03**

COURSE OBJECTIVES

This course will enable the students to:

1. Understand and Explain the software development perspective to the challenges of engineering software systems that are secure.
2. This course addresses design and implementation issues critical to producing secure software systems.
3. Gain knowledge about Software Assurance Model
4. To understand Identification and authentication in Software Security in Enterprise Business.
5. To learn about how Security development frameworks organized.

COURSE OUTCOMES:

1. Understand various aspects and principles of software security.
2. Devise security models for implementing at the design level.
3. Identify and analyze the risks associated with s/w engineering and use relevant models to mitigate the risks.
4. Understand the various security algorithms to implement for secured computing in enterprise Business and computer networks.
5. Explain different security frameworks for different types of systems including electronic systems

Course Content:-

UNIT –I

Introduction Defining computer security, the principles of secure software, trusted computing base, etc, Fundamentals of Threat Modeling, advanced techniques for mapping security requirements into design specifications. Secure software implementation, deployment and ongoing management.

UNIT -II

Software design and an introduction to hierarchical design representations. Difference between high-level and detailed design. Handling security with high-level design. General Design Notions. Security concerns designs at multiple levels of abstraction, Design patterns, quality assurance activities and strategies that

support early vulnerability detection, Trust models, security Architecture & design reviews.

UNIT -III

Software Assurance Model: Identify project security risks & selecting risk management strategies, Risk Management Framework, Security Best practices/ Known Security Flaws, Architectural risk analysis, Security Testing & Reliability. Introduction to reliability engineering, software reliability, Software Reliability approaches, Software reliability modeling.

UNIT -IV

Softwar**e** Security in Enterprise Business: Identification and authentication, Enterprise Information Security, Symmetric and asymmetric cryptography, including public key cryptography, data encryption standard (DES), advanced encryption standard (AES), SIEM/SOC, algorithms for hashes and message digests. Authentication, authentication schemes , access control models, Kerberos protocol, public key infrastructure (PKI), firewalls and VPNs.

UNIT –V

Security development frameworks. Security issues associated with the development and deployment of information systems, including Internet-based e-commerce, e-business, and eservice systems, as well as the technologies required to develop secure information systems for enterprises, policies and regulations essential to the security of enterprise information systems.

TEXT BOOKS:

1. W. Stallings, Cryptography and network security: Principles and practice, 5 th Edition, Upper Saddle River, NJ: Prentice Hall., 2011
2. C. Kaufman, r. Perlman, & M. Speciner, Network security: Private communication in a public world, 2 nd Edition, Upper Saddle River, NJ:Prentice HalL, 2002
3. C. P. Pfleeger, S. L. Pfleeger, Security in Computing, 4 th Edition, Upper Saddle River, NJ:Prentice Hall, 2007
4. M. Merkow, & J. Breithaupt, Information security: Principles and practices. Upper Saddle River, NJ:Prentice Hall, 2005

REFERENCE BOOKS:

Gary McGraw, Software Security: Building Security In, Addison-Wesley, 2006

Syllabus

Open Source Intelligence (CYT-120)

L:T:P:: 3:0:0 **Credits-03**

Course Description:

This course provides a comprehensive overview of Open Source Intelligence (OSINT) techniques and tools used to gather, analyze, and interpret information from publicly available sources. Students will learn how to effectively collect and evaluate data from various online and offline sources to support decision-making, investigations, and research.

Prerequisites:

Basic computer literacy and familiarity with internet browsing.

Unit 1: Introduction to Open Source Intelligence-Definition and scope of Open Source Intelligence (OSINT), Importance of OSINT in intelligence gathering and decision-making, Legal and ethical considerations in OSINT operations

Unit 2: OSINT Methodologies and Techniques- OSINT collection methods: passive vs. active reconnaissance,Searching techniques for gathering information from the web,Social media intelligence (SOCMINT) and online community analysis

Unit 3: OSINT Tools and Resources-Overview of OSINT tools and platforms, Search engines, web scraping tools, and data mining techniques, Using social media monitoring tools and analytics platforms

Unit 4: Analysis and Interpretation of OSINT Data- Data validation and verification techniques, Analyzing patterns, trends, and relationships in OSINT data, Visualization tools and techniques for presenting OSINT findings

Unit 5: Advanced OSINT Techniques-Deep web and dark web intelligence gathering, Geospatial intelligence (GEOINT) and mapping tools, Advanced online investigation techniques: OSINT automation and scripting

Textbook:

- "Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information" by Michael Bazzell

Syllabus

CLOUD SECURITY (CYT-121)

L:T:P:: 3:1:0 **Credits-04**

Course Objectives:

1. Understand the fundamental concepts of cloud security, including authentication, authorization, encryption, and access control.
2. Explore the various threats and vulnerabilities specific to cloud environments, such as data breaches, insider threats, and DDoS attacks.
3. Learn best practices for designing, implementing, and managing secure cloud architectures across different cloud service models (IaaS, PaaS, SaaS).
4. Gain practical skills in assessing and mitigating risks associated with cloud deployments through hands-on labs and case studies.
5. Develop strategies for continuous monitoring, compliance management, and incident response to ensure the ongoing security of cloud-based systems.

Course Outcomes:

1. Demonstrate proficiency in identifying and analyzing security risks within cloud infrastructures.
2. Implement appropriate security controls to protect data and resources in cloud environments.
3. Evaluate cloud service providers and select the most suitable options based on security requirements.
4. Design resilient cloud architectures that prioritize security, scalability, and reliability.
5. Communicate effectively about cloud security principles and practices to stakeholders, including executives, IT teams, and end users.

Unit 1: Introduction to Cloud Computing and Security

- Overview of cloud computing: definition, characteristics, deployment models (public, private, hybrid), service models (IaaS, PaaS, SaaS)
- Importance of security in cloud computing
- Key security challenges in cloud computing: data breaches, data loss, insider threats, compliance issues
- Cloud security architecture: shared responsibility model, layers of security (physical, network, host, application, data)
- Legal and regulatory considerations in cloud computing: GDPR, HIPAA, PCI DSS

Unit 2: Cloud Security Fundamentals

- Authentication and access control in the cloud: identity management, multi-factor authentication (MFA), role-based access control (RBAC), least privilege principle
- Data encryption: encryption at rest and in transit, key management, cryptographic protocols (TLS/SSL, AES)
- Network security in the cloud: virtual private cloud (VPC), network segmentation, firewall configuration, intrusion detection and prevention systems (IDPS)
- Security monitoring and logging: log management, security information and event management (SIEM), incident response procedures

Unit 3: Securing Cloud Infrastructure

- Securing cloud infrastructure components: virtual machines, containers, storage, databases
- Secure configuration management: hardening virtual machines, patch management, vulnerability scanning
- Container security best practices: image scanning, runtime protection, container orchestration security (e.g., Kubernetes)
- Data protection in the cloud: data classification, data masking, data loss prevention (DLP), backup and disaster recovery

Syllabus

Unit 4: Cloud Application Security

- Secure software development in the cloud: secure coding practices, DevSecOps, continuous integration and continuous deployment (CI/CD) pipelines
- API security: authentication and authorization, API gateway security, API rate limiting, input validation
- Web application security: OWASP Top 10 vulnerabilities, web application firewalls (WAF), secure session management, content security policies (CSP)

Unit 5: Compliance, Governance, and Risk Management

- Cloud compliance frameworks: SOC 2, ISO/IEC 27001, NIST Cybersecurity Framework
- Cloud governance: policies, procedures, standards, and guidelines for cloud usage
- Risk management in the cloud: risk assessment methodologies, risk mitigation strategies, risk monitoring and reporting
- Cloud audit and assurance: conducting cloud security audits, third-party risk assessment, compliance reporting

TEXTBOOKS

1. "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance" by Tim Mather, Subra Kumaraswamy, and Shahed Latif - This book provides a comprehensive overview of cloud security issues and strategies from an enterprise perspective.
2. "Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)" by Michael J. Kavis - While not solely focused on security, this book delves into the architectural considerations of cloud computing, including security implications for various service models.
3. "Cloud Computing Security: Foundations and Challenges" edited by John R. Vacca - This book covers foundational concepts and challenges in cloud security, offering insights into both theoretical and practical aspects of securing cloud environments.

Syllabus

REVERSE ENGINEERING MALWARE: MALWARE ANALYSIS TOOLS AND TECHNIQUES LAB (CYP-109)

L:T:P:: 0:0:2 **Credits-01**

Course Objectives:

1. Understand the fundamental concepts and principles of malware analysis.
2. Familiarize students with various types of malware and their behavior.
3. Provide hands-on experience with malware analysis tools and techniques.
4. Develop skills in static and dynamic analysis of malicious code.
5. Cultivate an understanding of the threat landscape and the importance of continuous learning in cybersecurity.

Course Outcomes:

1. Students will be able to analyze different types of malware using both static and dynamic analysis methods.
2. Students will gain proficiency in using popular malware analysis tools such as IDA Pro, OllyDbg, and Wireshark.
3. Students will develop the ability to identify and classify malware based on its characteristics and behavior.
4. Students will be able to create detailed malware analysis reports, documenting their findings and insights.
5. Students will understand the importance of ethical considerations and legal constraints in malware analysis and reverse engineering practices.

1. **Static Analysis**:
    - Identifying file properties (e.g., file type, size, entropy).
    - Extracting strings from the malware sample.
    - Examining file headers and metadata.
    - Identifying and analyzing embedded resources (e.g., executables, DLLs).
    - Identifying potential indicators of compromise (IOCs) in the binary.
2. **Dynamic Analysis**:
    - Running the malware sample in a controlled environment (e.g., sandbox).
    - Monitoring system calls and API calls made by the malware.

- Capturing network traffic generated by the malware (if any).
- Analyzing the behavior of the malware (e.g., file system modifications, registry changes, process creation).

3. **Code Analysis**:
   - Disassembling the malware sample to analyze its assembly code.
   - Identifying and analyzing key functions (e.g., encryption/decryption routines, network communication).
   - Tracing execution flow to understand the malware's functionality.
   - Identifying anti-analysis techniques employed by the malware (e.g., obfuscation, packing).
4. **Memory Analysis**:
   - Analyzing volatile memory (RAM) to identify running processes and their associated memory regions.
   - Examining process memory to identify injected code or malicious payloads.
   - Identifying artifacts of malware execution in memory (e.g., hooks, injected DLLs).
5. **Behavioral Analysis**:
   - Analyzing system logs and monitoring tools to identify suspicious behavior.
   - Correlating findings from static and dynamic analysis to understand the full scope of the malware's capabilities.
   - Documenting and reporting findings, including potential indicators of compromise and mitigation recommendations.
6. **Reverse Engineering Techniques**:
   - Using debuggers and disassemblers to analyze the malware's code.
   - Employing techniques such as code patching and hooking to modify malware behavior for analysis purposes.
   - Identifying and bypassing anti-analysis mechanisms employed by the malware.
7. **Malware Classification**:
   - Classifying the malware sample based on its behavior, characteristics, and purpose.
   - Comparing the malware sample to known malware families or threat intelligence databases.

Syllabus

CLOUD SECURITY LAB (CYP-110)

L:T:P:: 0:0:2 **Credits-01**

Course Objectives:

1. Understand fundamental concepts of cloud computing security, including shared responsibility models, encryption mechanisms, and access control.
2. Gain hands-on experience with cloud security tools and techniques for monitoring, detecting, and mitigating security threats in cloud environments.
3. Develop skills in configuring and managing cloud security services such as identity and access management (IAM), network security groups, and security information and event management (SIEM) systems.
4. Explore advanced topics in cloud security, such as container security, serverless security, and securing cloud-native applications.
5. Analyze real-world cloud security incidents and breaches, and develop incident response plans and strategies for effectively mitigating and recovering from security incidents in the cloud.

Course Outcomes:

1. Demonstrate proficiency in assessing and mitigating security risks associated with cloud computing deployments, including infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) models.
2. Implement security best practices for securing cloud workloads, data, and applications, including encryption, key management, and secure data transfer protocols.
3. Configure and manage cloud security controls and compliance frameworks to meet regulatory requirements and industry standards such as GDPR, HIPAA, and PCI DSS.
4. Apply threat intelligence and security monitoring techniques to detect and respond to security incidents and anomalies in cloud environments.
5. Communicate effectively with stakeholders, including IT teams, management, and end-users, to ensure a comprehensive understanding of cloud security risks and mitigation strategies.

1. **Cloud Service Configuration Analysis**:
    - Analyzing the configuration settings of cloud services (e.g., AWS, Azure, Google Cloud) to identify security vulnerabilities.
    - Assessing access controls, encryption settings, and network configurations for potential

misconfigurations.

2. **Cloud Identity and Access Management (IAM) Analysis**:
    - Examining IAM policies and roles to ensure least privilege access and proper segregation of duties.
    - Conducting a permissions audit to identify over-permissioned accounts or roles.
3. **Data Encryption and Key Management**:
    - Analyzing data encryption mechanisms used to protect data at rest and in transit within the cloud environment.
    - Evaluating key management practices to ensure secure storage and rotation of encryption keys.
4. **Cloud Network Security**:
    - Analyzing network security groups, firewall rules, and virtual private cloud (VPC) configurations to identify potential security gaps.
    - Assessing network traffic logs and monitoring tools to detect and respond to suspicious network activity.
5. **Logging and Monitoring Analysis**:
    - Reviewing cloud provider logs (e.g., AWS CloudTrail, Azure Activity Log) to identify security incidents and unauthorized access attempts.
    - Setting up and configuring cloud monitoring tools to detect anomalous behavior and potential security breaches.
6. **Incident Response Simulation**:
    - Simulating a cloud security incident (e.g., unauthorized access, data breach) and responding to it according to established incident response procedures.
    - Conducting post-incident analysis to identify root causes and lessons learned for improving cloud security posture.
7. **Cloud Compliance Assessment**:
    - Assessing cloud environments against industry standards and regulatory requirements (e.g., GDPR, HIPAA, PCI DSS).
    - Conducting compliance audits and generating compliance reports to demonstrate adherence to security standards.
8. **Security Automation and Orchestration**:

- Implementing security automation scripts or workflows to enforce security policies, automate routine tasks, and streamline incident response processes.
- Integrating security tools and services with cloud provider APIs for automated threat detection and response.

9. **Cloud Security Best Practices Review**:
    - Reviewing cloud security best practices and guidelines provided by cloud service providers and industry organizations.
    - Identifying gaps in current security practices and implementing recommendations for improving cloud security posture.
10. **Cloud Penetration Testing**:
    - Conducting penetration tests against cloud environments to identify security vulnerabilities and weaknesses.
    - Performing vulnerability scans, exploitation, and privilege escalation exercises to assess the effectiveness of cloud security controls.

Syllabus

OPEN-SOURCE INTELLIGENCE LAB (CYP-111)

L:T:P:: 0:0:2 **Credits-01**

Course Outcomes:

Student will be able to:

1. Perform a variety of OSINT investigations while practicing good OPSEC, Create sock puppet accounts and Locate information on the internet, including some hard-to-find and deleted information
2. Locate individuals online and examine their online presence
3. Understand and effectively search the dark web and Create an accurate report of the online infrastructure for cyber defense, merger and acquisition analysis, pen testing, and other critical areas for an organization.
4. Use methods that can often reveal who owns a website as well as the other websites that they own or operate and Understand the different types of breach data available and how they can be used for offensive and defensive purposes
5. Effectively gather and utilize social media data, Understand and use facial recognition and facial comparison engines, Quickly and easily triage large datasets to learn what they contain and Identify malicious documents and documents designed to give away your location

1: OSINT and OPSEC Fundamentals

Exercises

- Managing Your Attribution
- Dealing with Potential Malware
- Canary Tokens
- Hunchly
- Obsidian
- [Optional] Linux Command Line Practice

2:Essential OSINT Skills

Exercises

- Search
- Instant Data Scraper
- Metadata
- Reverse Image Search
- Facial Recognition
- Translation

3: Investigating People

Exercises

- Researching Usernames
- Keybase
- Email
- Twitter
- Twitter Bot Analysis

4: Investigating Websites and Infrastructure

Exercises

- IP Address Research
- WHOIS
- DNS
- Amass and Eyewitness
- Censys and Shodan
- Buckets of Fun

5: Automation, the Dark Web, and Large Data Sets

Exercises

- Business
- Wireless
- Bulk Data Triage
- Tor and PGP
- Breach Data

6: Capstone: Capture the Flag

The GIAC Open Source Intelligence (GOSI) certification confirms that practitioners have a strong foundation in OSINT methodologies and frameworks and are well-versed in data collection, reporting, and analyzing targets.

- Open Source Intelligence Methodologies
- OSINT Data Collection, Analysis, and Reporting
- Harvesting Data from the Dark Web
- Operational Security Fundamentals and Consideration

Syllabus

DESIGN PROJECT (CYP-112)

L:T:P:: 0:0:4 **Credits-02**

COURSE OBJECTIVES: The objectives of the course are to

3. Develop skills in doing literature survey, technical presentation, and report preparation.
4. Enable project identification and execution of preliminary works on final semester project.

COURSE OUTCOMES: On successful completion of this course, the students shall be able to

6. Discover potential research areas in the field of information technology.
7. Create very precise specifications of the IT solution to be designed.
8. Have introduction to the vast array of literature available about the various research challenges in the field of IT.
9. Use all concepts of IT in creating a solution for a problem.
10. Have a glimpse of real world problems and challenges that need IT-based solutions.

Syllabus

MINI PROJECT-III/ INTERNSHIP-III(CYP-113)

L:T:P:: 0:0:2 **Credits-01**

ABOUT INTERNSHIP/MINI PROJECT

It is an organized method or activity of enhancing and improving engineering students' skill sets and knowledge, which boosts their performance and consequently helps them meet their career objectives. Industrial Training is essential in developing the practical and professional skills required for an Engineer and an aid to prospective employment.

OBJECTIVES OF INTERNSHIP/MINI PROJECT:

1. The main objective of the internship/mini projectis to expose the students to the actual working environment and enhance their knowledge and skill from what they have learned in college.
2. Another purpose of this program is to enhance the good qualities of integrity, responsibility, and self-confidence. Students must follow all ethical values and good working practices.
3. It is also to help the students with the safety practices and regulations inside the industry and to instils the spirit of teamwork and good relationship between students and employees.

COURSE OUTCOMES: At the end of internship/mini project, the students will be able to

1. Understand organizational issues and their impact on the organization and employees.
2. Identify industrial problems and suggest possible solutions.
3. Relate, apply and adapt relevant knowledge, concepts and theories within an industrial organization, practice and ethics.
4. Apply technical knowledge in an industry to solve real world problems.
5. Demonstrate effective group communication, presentation, self-management, and report writing skills