G H Raisoni College of Engineering & Management, Nagpur

(An Autonomous Institute affiliated to RTM Nagpur University Nagpur)

B. Tech. in Computer Science & Engineering (Cyber Security)

With Multidisciplinary Minor (MDM)

UG Scheme & Curriculum - 2023 (NEP 2020)

G H Raisoni College of Engineering & Management
(Formerly Known as G H Raisoni Institute of Engineering &Technology, Nagpur)
An Autonomous Institute Affiliated to Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur
Accredited by NAAC with "A+" Grade
Shraddha Park, B-37-39/1, MIDC, Hingna-Wadi Link Road, Nagpur-440016 (INDIA)

UG Scheme-2023 (NEP-2020)

B. Tech. CSE (Cyber Security)

Semester	Credits	Hours	Marks	Theory Heads	Practical Heads	Total Heads
I	20	27	600	7	6	13
II	20	26	550	6	5	11
III	20	21	550	6	2	8
IV	20	23	600	8	3	11
V	22	27	550	6	4	10
VI	22	28	600	6	5	10
VII	22	28	575	5	3	8
VIII	16	28	375	1	1	2
Total	**162**	**204**	**4400**	**45**	**29**	**73**

Department of Computer Science & Engineering (Cyber Security)

Scheme Summary

Course Category Credits Summary

SEMESTER		I	II	III	IV	V	VI	VII	VIII	TOTAL
Basic Science Course	BSC/ESC	6	8							14
Engineering Science Course		8	4							12
Program Core Course	PCC/PEC		2	8	8	10	8	10		46
Program Elective Course						4	8	4	4	20
Multidisciplinary Minor	MDC			2	2	4	2	4		14
(Open elective Course)				4	2	2				8
Vocational & Skill Course	Skill C	2	2		2		2			8
Ability Enhancement Courses	HSSMC	2			2					4
Entrepreneurship/Economics/ Management Courses				2	2					4
Indian Knowledge System			2							2
Value Education Courses				2	2					4
Research Methodology	ELC					2	2			4
Comm. Engg Project /Field Project				2						2
Project								4		4
Internship/OJT									12	12
Co-curricular Courses	LLC	2	2							4
Total credits		20	20	20	20	22	22	22	16	162

Department of Computer Science & Engineering (Cyber Security)

B. Tech.CSE (Cyber Security)

Course Code	Name of Course	Course Category	Teaching Scheme				Credits	Evaluation Scheme					
								Theory			Practical		Total Marks
			L	T	P	Total Hours		TAE	CAE	ESE	INT	EXT	
SEMESTER-I													
23BTSHL101CY 23BTSHP101CY	Engineering Physics	BSC2	1	1	2	4	3	10	15	50	25	-	100
23BTSHL103CY	Matrices and Differential Calculus	BSC1	2	1	-	3	3	10	15	50	-	-	75
23BTSHL108CY 23BTSHP108CY	Communication Skills	AEC1	1	-	2	3	2	10	15		25	-	50
23BTSHL10XCY	Elective: Indian Knowledge System	IKS	2	-	-	2	2	10	15	50			75
23BTSHP112CY	Liberal Learning Courses-I	CC1	-	-	4	4	2	-	-	-	25	25	50
23BTCYL101 23BTCYP101	Introduction to Cyber Security.	PCC1	1	-	2	3	2	10	15	50	25	-	100
23BTCYL10X 23BTCYP10X	Elective -I: Vocational and Skill Enhancement	VSEC1	1	-	2	3	2	10	15		25	-	50
23BTITL102CY 23BTITP102CY	Programming for Problem Solving	ESC3	3	-	2	5	4	10	15	50	25	-	100
TOTAL			**11**	**2**	**14**	**27**	**20**	**70**	**105**	**250**	**150**	**25**	**600**

Department of Computer Science & Engineering (Cyber Security)

Course Code	Name of Course	Course Category	Teaching Scheme				Credits	Evaluation Scheme					
								Theory			Practical		Total Marks
			L	T	P	Total Hours		TAE	CAE	ESE	INT	EXT	
SEMESTER-II													
23BTSHL102CY 23BTSHP102CY	Environmental Chemistry	BSC5	1	-	2	3	2	10	15	50	25	-	100
23BTSHL104CY	Integral Calculus and Differential Equations	BSC3	2	1	-	3	3	10	15	50	-	-	75
23BTSHL105CY	Linear Algebra and Statistics	BSC4	2	1	-	3	3	10	15	50	-	-	75
23BTSHP113CY	Liberal Learning Courses-II	CC2	-	-	4	4	2	-	-	-	25	25	50
23BTEEL101CY 23BTEEP101CY	Basic Electrical Engineering	ESC1	3	-	2	5	4	10	15	50	25	-	100
23BTECL101CY 23BTECP101CY	Digital Logic Design	ESC2	3	-	2	5	4	10	15	50	25	-	100
23BTCYL10X 23BTCYP10X	Elective –II: Vocational and Skill Enhancement	VSEC 2	1	-	2	3	2	10	15		25	-	50
TOTAL			**12**	**2**	**12**	**26**	**20**	**60**	**90**	**250**	**125**	**25**	**550**

ELECTIVES

23BTSHL10XCY -Elective: Indian Knowledge System -

Course	Course Code (L)	Course Code(P)
Elective: IKS-1- Concepts and Applications in Engineering	**23BTSHL109CY**	**Not Applicable**
Elective: IKS-2- Social History of Medicine In Colonial India	**23BTSHL110CY**	**Not Applicable**
Elective: IKS-3- Modern IndianArchitecture	**23BTSHL111CY**	**Not Applicable**

CYB Board

Course	Course Code (L)	Course Code(P)
Elective -I :Vocational and Skill Enhancement -	23BTCYL102	23BTCYP102
Elective -I :Vocational and Skill Enhancement-	23BTCYL103	23BTCYP103
Elective -I :Vocational and Skill Enhancement-	23BTCYL104	23BTCYP104
Elective –II: Vocational and Skill Enhancement-	23BTCYL105	23BTCYP105
Elective –II: Vocational and Skill Enhancement	23BTCYL106	23BTCYP106
Elective –II: Vocational and Skill Enhancement-	23BTCYL107	23BTCYP107

Department of Computer Science & Engineering (Cyber Security)

Course Code	Name of Course	Course Category	Teaching Scheme				Credits	Evaluation Scheme					
								Theory			Practical		Total Marks
			L	T	P	Total Hours		TAE	CAE	ESE	INT	EXT	
SEMESTER-III													
BSBTSH4TT321CY	Discrete Mathematics and Graph Theory	PCC2	3	1		4	4	10	15	50	-	-	75
BTCS3TT301CY	Data Structures and Algorithms	PCC3	3	-	-	3	4	10	15	50	-	-	75
BTCS1PT301CY	Data Structures and Algorithms	PCC3	-	-	2	2		-	-	-	25	25	50
BTCY2TT301	Multi-Disciplinary	MD1	2			2	2	10	15	50			75
BTCY2TT302	Open elective -I	OE1	4			4	4	10	15	50			75
HMBTMBL301CY	Engineering Economics and Industrial Management	EEMC1	2			2	2	10	15	50			75
VEBTSH2TTXXXCY	Humanities Elective	VEC1	2			2	2	10	15	50			75
BTCY2PI303	Project –I (NGO)	CEP			2	2	2				50		50
TOTAL			**16**	**1**	**4**	**21**	**20**	**60**	**90**	**300**	**75**	**25**	**550**

For Multi-Disciplinary from others:
CSE: - Computer Architecture

AI: - Knowledge Representation ……

DS: - Fundamentals Data Science

Open Elective – I: - Web Cloud Computing Application: BTCY2TT302

MD1: Cyber Law: BTCY2TT301(TO OTHERS)

MD1: Fundamentals Data Science (For Cyber)

Department of Computer Science & Engineering (Cyber Security)

Course Code	Name of Course	Course Category	Teaching Scheme				Credits	Evaluation Scheme					
								Theory			Practical		Total Marks
			L	T	P	Total Hours		TAE	CAE	ESE	INT	EXT	
SEMESTER-IV													
23BTCSL204CY	Database Management Systems	PCC4	3			3	4	10	15	50	-	-	75
23BTCSP204CY	Database Management Systems	PCC4			2	2		-	-	-	25	25	50
23BTCYL204	Computer Architecture and Operating System	PCC5	4			4	4	10	15	50			75
23BTXXXX	Multi-Disciplinary	MD2	2			2	2	10	15	50			75
23BTXXXX	Open elective -II	OE2	2			2	2	10	15	50			75
23BTXXXX	Skill Enhancement Course -III:	VSEC3	1	-	2	3	2	10	15		25	-	50
23BTSHL231CY	Aptitude & Employability Skills :2	AEC2	1	-	2	3	2	10	15		25	-	50
23BTMBL202CY	EDP	EEMC2	2	-		2	2	10	15	50		-	75
23BTSHL233CY	Universal Human Values 2: Understanding Harmony	VEC2	2			2	2	10	15	50			75
TOTAL			**17**	**0**	**6**	**23**	**20**	**80**	**120**	**300**	**75**	**25**	**600**

MD2: - Cyber Crimes and Investigation: 23BTCYL205
Open Elective: - OE-II: Web Security: - 23BTCYL206

VSEC3: -Skill Enhancement Course -III:

Principles of Object Oriented Programming - VSEC3: 23BTCYL207 / 23BTCYP207

Security in IoT –VSEC3: 23BTCYL208 / 23BTCYP208

Department of Computer Science & Engineering (Cyber Security)

Course Code	Name of Course	Course Category	Teaching Scheme				Credits	Evaluation Scheme					
								Theory			Practical		Total Marks
			L	T	P	Total Hours		TAE	CAE	ESE	INT	EXT	
SEMESTER-V													
23BTCYL301	Fundamentals of Cryptography	PCC6	3	1	-	4	4	10	15	50	-	-	75
23BTCYL302	Cyber Laws & Ethics	PCC7	3	-	-	3	3	10	15	50	-	-	75
23BTCYL303	Intro.to Penetration Testing	PCC8	2	-	-	4	3	10	15	50	-	-	75
23BTCYP303	Intro.to Penetration Testing	PCC8	-	-	2			-	-	-	25	-	25
23BTCYLXXX	PE-I	PEC1	3	-	-	3	4	10	15	50	-	-	75
23BTCYPXXX	PE-I	PEC1	-	-	2	2		-	-	-	25	-	25
23BTXXXX	Multi-Disciplinary	MDM3	3	-	2	5	4	10	15	50	25	-	100
23BTXXXX	Open elective -III	OE3	2	-	-	2	2	10	15	50			75
23BTSHP301CY	Research Methodology	RM	-	-	4	4	2	-	-	-	25	-	25
TOTAL			**16**	**1**	**10**	**27**	**22**	**60**	**90**	**300**	**100**		**550**

MDM3: Computer Security: 23BTCYL307

OE3: Principles of Cryptography: 23BTCYL308

PE-I: Ethical Hacking: 23BTCYL304/23BTCTP304

PE-1: AI For IoT Applications: 23BTCYL305/23BTCYP305

Department of Computer Science & Engineering (Cyber Security)

Course Code	Name of Course	Course Category	Teaching Scheme				Credits	Evaluation Scheme					
								Theory			Practical		Total Marks
			L	T	P	Total Hours		TAE	CAE	ESE	INT	EXT	
SEMESTER-VI													
23BTCYL310	Principles of Algorithm Design	PCC9	3			3	4	10	15	50			75
23BTCYP310	Principles of Algorithm Design	PCC9	-	-	2	2		-	-	-	25	25	50
23BTCYL312	Data Analytics	PCC10	3			3	4	10	15	50	-	-	75
23BTCYP312	Data Analytics	PCC10			2	2		-	-	-	25	25	50
23BTCYLXXX	PE-II	PEC2	3		-	3	4	10	15	50			75
23BTCYPXXX	PE-II	PEC2	-	-	2	2		-	-	-	25		25
23BTCYLXXX	PE-III	PEC3	4			4	4	10	15	50			75
23BT3XXXX	Multi-Disciplinary	MD4	2			2	2	10	15	50			75
23BTXXXXX	Skill Enhancement Course -IV	VSEC4	1	-	2	3	2	10	15		25	-	50
23BTSHP302CY	Research Ethics & Technical Writing	RM	-	-	4	4	2	-	-	-	50	-	50
TOTAL			16		12	28	22	60	90	250	150	50	600

PE-II: 1. Web Application Security (23BTCYL315/ 23BTCYP315)
2. IOT using Robotics (23BTCYL317/ 23BTCYP317)

PE-III: 1. Digital Forensics (23BTCYL321)
2. Privacy and Security in IOT/OT (23BTCYL323)

MD4(To *Other Dept.*): Network Security (23BTCYL313)

VSEC-IV: Information Coding Technique (23BTCYL308/23BTCYP308)

Department of Computer Science & Engineering (Cyber Security)

Course Code	Name of Course	Course Category	Teaching Scheme				Credits	Evaluation Scheme					
								Theory			Practical		Total Marks
			L	T	P	Total Hours		TAE	CAE	ESE	INT	EXT	
SEMESTER-VII													
23BTCYL401	Applied Cyber Security	PCC11	3		-	3	4	10	15	50	-	-	75
23BTCYP401	Applied Cyber Security Lab	PCC11	-	-	2	2		-	-	-	25	25	50
23BTCYL403	Advance Information Security	PCC12	3			3	3	10	15	50			75
23BTCYL404	Web Technology	PCC13	2		-	2	3	10	15	50	-	-	75
23BTCYP404	Web Technology	PCC13	-	-	2	2		-	-	-	25	25	50
23BTCYLXXX	PE-IV	PEC4	4			4	4	10	15	50			75
23BTXXXXXX	Multi-Disciplinary	MD5	4			4	4	10	15	50			75
23BTCYP431	Project	P			8	8	4				50	50	100
TOTAL			**16**		**12**	**28**	**22**	**50**	**75**	**250**	**100**	**100**	**575**

MD5: (Other Branch): CTIF
MD5: Python Programming (Cyber)
PE-IV -1: Computer Vision
PE-IV-2: EAR

Department of Computer Science & Engineering (Cyber Security)

Course Code	Name of Course	Course Category	Teaching Scheme				Credits	Evaluation Scheme					
								Theory			Practical		Total Marks
			L	T	P	Total Hours		TAE	CAE	ESE	INT	EXT	
SEMESTER-VIII													
23BTCYL4XX	PE-V (MOOCs based)	PEC5	4			4	4	10	15	50			75
23BTCYP418	Internship	I			24	24	12				200	100	300
TOTAL			**4**		**24**	**28**	**16**	**10**	**15**	**50**	**200**	**100**	**375**

SEMESTER-III

Course Title: Discrete Mathematics and Graph Theory										
Semester	III	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	ODD	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PCC2	3	1	--	4	10	15	50	--	--
Course Code	BSBTSH4T T321CY									
Teaching Mode	Offline	4			Total	75			--	
Duration of ESE	3 hrs					75				

Course Objectives	This course introduces concepts of set theory and graph theory and its application to computer science.
	It also skills to analyze various kinds of sets and groups of objects meeting the criteria.
	It also introduces combinatorial structures and applies algebraic techniques to combinatorial problems.
Course Outcomes	**CO1**: Know grouping of objects and operation, relation, ordering of objects, concepts of Groups.
	CO2: Classify the algebraic structure for a given mathematical problem.
	CO3: Apply the concept of Boolean algebra in computer science engineering.
	CO4: Solve problems using basic graph theory.
	CO5: Develop algebraic technique to solve combinatorial problems using combinatorial structure.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1	**3**	**3**										**3**			
CO2	**3**	**3**										**3**			
CO3	**3**	**3**										**3**			
CO4	**3**	**3**										**3**			
CO5	**3**	**3**										**3**			
CO6	**3**	**3**										**3**			

Department of Computer Science & Engineering (Cyber Security)

Course Contents:

Unit	Contents	Hours
I	**Set Theory** Operations on sets, Laws of algebra of sets, Representation of sets on computer in terms of 0's & 1's. Partition & covering of a set, ordered pair, Product set, Relation– Different types of relations, Graph of relation, Matrix of relation, Transitive closure of relation, Properties of relations, Compatible relation. Functions, Partial ordering & partially ordered set, Hasse diagram of Poset, Totally ordered set, Peano axioms & Mathematical Induction.	10
II	**Group** Algebra or Algebraic systems like semigroup, monoid and examples. Homomorphism, Isomorphism of semigroup & monoid. Groups, properties of algebraic groups. Permutations groups, Subgroups, Cosets, Lagrange's theorem, properties of cyclic groups, generator of group, kernel of Homorphism, quotient group, Rings, types of rings, Fields, subring, Integral domain.	8
III	**Lattices and Boolean algebra** Lattice as Poset & as algebraic system, Types of lattices, Hasse diagrams, Sublattice, direct product of Lattices, Lattice Homomorphism, complement of elements of lattices, Various lattices, composition tables, Lattice, Boolean algebra; Boolean Expressions, Equivalence of Boolean Expression by tables, Simplification of circuit & equivalent circuit by truth tables.	8
IV	**Graph Theory** Graphs and its types, Sub graph, Quotient graph, Euler path, complete path, indegree, outdegree, reachability, cycle, matrix representation of graph. Transitive closure of graph, Adjacency matrix, Trees, Venn diagram, Representation of trees, binary trees, spanning trees, Prim's algorithm.	8
V	**Combinatorics** Counting Theorem and application, multiplication principle of counting, Permutation & Combination with examples, Definition of generating functions and it's examples, proof of simple combinatorial identities. Recursive relations: definitions & examples, explicitly formula for sequence, back tracking to find explicit formula of sequence, Solving recurrence relations. The pigeon hole principle & extended pigeon hole principle and application of pigeon hole principle in solving simple problems.	8

Text Books	1.	Discrete Mathematical structure with application to computer science by Trembley & Manohar (Mc. Graw Hill)
	2.	Discrete Mathematical Structure by Kolmann , Busby & Ross (PHI)
	3.	Discrete mathematics by Lipschutz & Lipson , Schaum's outline, TMH
Reference Books	1.	Discrete Mathematics by Liu
	2.	Discrete Mathematics by John Truss (Addison Wesley, 2000)
	3.	Foundations of Discrete Mathematical by K. D. Joshi (Willey Eastern).

Course Title: **Data Structure and Algorithms**										
Semester	III	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	ODD	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PCC3	3	--	2	4	10	15	50	25	25
Course Code	BTCS3TT301CY/BTCS1PT301CY									
Teaching Mode	Offline	5			Total	75			50	
Duration of ESE	3 HRS					125				

Course Objectives	This course introduces basic idea of data structure while making aware of methods and structure used to organize large amount of data.
	It's also aimed at developing skill to implement methods to solve specific problems using basic data structures.
	The course also provides career opportunities in design of data, implementation of data, technique to sort and searching the data.
Course Outcomes	CO1: Analyze various techniques for searching, Sorting and Hashing.
	CO2: Illustrate linear arrays and linked lists, including operations such as insertion, deletion, traversal, sorting, and searching.
	CO3: Demonstrate the array and linked representations of stacks and queues and their applications.
	CO4: Apply trees as non-linear data structure to find solution for given engineering applications.
	CO5: Understand the basics of Graphs as non-linear data structures.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes													
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2
CO1		3	2	3									1	
CO2		2	3	3									2	
CO3		3	3	3									2	1
CO4		3	3	3									3	2
CO5		3	3	2									3	1

Course Contents:

Unit	Contents	Hours
I	Introduction to Algorithms, Searching and Sorting Introduction to Algorithms, Common operations on data structures, Types of data structures, Abstract Data Type Time and Space Complexity, Step Count Method, Asymptotic Notations. Searching: Linear Search, Binary Search Sorting: Bubble sort, Selection Sort, Merge-Sort, Shell Sort, Radix Sort, Introduction to Hashing	9
II	Arrays and Linked Lists Arrays: Introduction, Linear Arrays, Arrays as ADT, Representation of Linear array in Memory, Traversing Linear Arrays, Insertion and deletion in arrays. Linked List: Introduction, Representation of Linked Lists in Memory, Traversing a Linked List, Searching a Linked List, Memory Allocation; Garbage Collection, Types of linked lists, Insertion and Deletion in Singly Linked List, Insertion and Deletion in Doubly Linked List, Insertion and Deletion in Circular Linked List	9
III	Stacks, Queue and Recursion Stacks-Introduction to Stacks, Array Representation of Stacks ,Linked Representation of Stacks, Stack as ADT, Various operations on stacks using arrays and linked lists, Application of Stacks : Polish Notations, Recursion, Towers of Hanoi Queue: Introduction to Queues, Array Representation of Queues, Linked Representation of Queues, Queues as ADT, Circular Queues, Deques, Priority Queues, Applications of Queues	9
IV	Trees and Binary Trees General and Binary Trees, Representation of binary tree in memory, Operations on Binary Trees, Binary Tree Traversals, Threaded Binary Trees, Binary Search Trees, various operations in Binary Search Trees, AVL Search Trees, Insertion in an AVL Search Tree, Deletion in an AVL Search Tree, m-way Search Trees, B-Trees-Insertion and deletion in B-Tree, B+Trees-Insertion and deletion in B+Tree	10
V	Graphs and their Applications: Introduction, Graph Theory Terminology, Representation of Graphs, Operations on Graphs, Traversing a Graph, Posets , Topological Sorting, Spanning Trees, Minimum Spanning Trees	8

Text Books	1.	AVAho, J Hopcroft, JD Ullman, Data Structures and Algorithms, Addison-Wesley, 1983.
	2.	THCormen, CF Leiserson, RL Rivest, C Stein, Introduction to Algorithms, 3rd Ed., MIT Press, 2009.
	3.	Sahni, S., "Data Structures, Algorithms, and Applications in C++", WCB/McGraw-Hill.
E--Books	1.	https://apps2.mdp.ac.id/perpustakaan/ebook/Karya%20Umum/Dsa.pdf
Reference Books	1.	Data Structures & Algorithms, 1e, Alfred V.Aho, Jeffery D. Ullman , Person.
	2.	MT Goodrich, R Tamassia, DM Mount, Data Structures and Algorithms in Java, 5th Ed., Wiley, 2010. (Equivalent book in C also exists.)
	3.	Wirth, N., "Algorithms and Data Structures", Prentice-Hall of India.
On-line TL Material	1.	https://nptel.ac.in/courses/106/102/106102064/
	2.	http://cse01-iiith.vlabs.ac.in/
	3.	https://ds2-iiith.vlabs.ac.in/data-structures-2/

Name of Subject: Data Structures & Algorithms (BTCS1PT301CY)	
COURSE OUTCOME	
CO1	Students shall be able to Illustrate various technique to for searching, Sorting.
CO2	Students shall be able to Explain the significance of dynamic memory management Techniques.
CO3	Students shall be able to Demonstrate the array and linked representations of stacks and queues and their applications.
CO4	Students shall be able to Apply trees as non-linear data structure to find solution for given engineering applications.
CO5	Students shall be able to Understand the basics of Graphs as non-linear data structures.

List of Practical

Sr. No.	Practical List	Mapping With CO	Mapping With PO& PSO
1	Write a program to search an element using linear & binary search.	CO1	PO1, PO2, PO3, PO4, PO12 & PSO1, PSO3
2	Write a program to implement insertion sort.	CO1	PO1, PO2, PO3, PO4, PO12 & PSO1, PSO3
3	Write a program to insert & delete an element at any position in singly linked list.	CO2	PO1, PO2, PO3, PO4, PO12 & PSO1, PSO3
4	Write a program to insert & delete an element at any position in doubly linked list.	CO2	PO1, PO2, PO3, PO4, PO12 & PSO1, PSO3
5	Write a program to implement stacks and queues using arrays.	CO3	PO1, PO2, PO3, PO4, PO12 & PSO1, PSO3
6	Write a program to convert an infix expression to postfix using stacks.	CO3	PO1, PO2, PO3, PO4, PO12 & PSO1, PSO3
7	Write a program to find the inorder, preorder and postorder traversal of a binary tree.	CO4	PO1, PO2, PO3, PO4, PO12 & PSO1, PSO3
8	Write a program to implement Breadth First Search (BFS) and Depth first search (DFS) in graph.	CO5	PO1, PO2, PO3, PO4, PO12 & PSO1, PSO3
Practical Beyond Syllabus			
9	Implementation of Floyd Warshalls Algorithm	CO5	PO1, PO2, PO3, PO4, PO12 & PSO1, PSO3
Open Ended Practical			
10	Demonstrate the various operations of Binary Search Trees using Virtual Lab	CO4	PO1, PO2, PO3, PO4, PO12 & PSO1, PSO3

Department of Computer Science & Engineering (Cyber Security)

Course Title: Cyber Laws -NEP										
Semester	III	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	Odd	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	**MD1**	2	-	-	2	10	15	50	-	-
Course Code	BTCY2TT301									
Teaching Mode	Offline	2			Total	75			-	
Duration of ESE	3 Hr					75				

Course Objectives	To understand the basics need of Cyber laws
	To understand the ethical issues in Cyber Space
	To Understanding the initiatives taken by Government to incorporate Cyber Laws
Course Outcomes	Upon successful completion of this course, studsent will be able to: **CO1:** Understand cyberspace & legal issues in cyber society.
	CO2: Apply facets of India IT act.
	CO3: Analyze the intellectual property issues and development of the law in this regard.
	CO4: Design model for cyber-crime scenarios.
	CO5: Evaluate e-governance and digital evidence management

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1	--	1	--	--	--	3	--	2	--	--	--	--	2	--	2
CO2	--	2	--	--	--	3	--	3	--	--	--	1	2	--	2
CO3	--	--	--	--	--	3	--	2	--	--	--	1	--	3	--
CO4	--	--	--	3	3	1	--	2	--	--	--	--	2	--	--
CO5	--	--	--	--	--	3	--	2	--	--	--	1	--	3	2

Course Contents:

Unit	Contents	Hours
I	**Introduction to Cyber law:** Evolution of computer Technology, emergence of cyber space. Cyber Jurisprudence, Need for IT act – Cyberspace-Web space, Web hosting and web Development agreement, Legal and Technological Significance of domain Names, Internet as a tool for global access.	4
II	**The Indian IT Act**, Challenges to Indian Law and Cybercrime Scenario in India, Cybercrime and Punishment, Network Service Providers Liability.	4
III	**DATA PROTECTION AND PRIVACY CONCERNS IN CYBERSPACE** Need to protect data in cyberspace Types of data Legal framework of data protection Data protection bill -an overview GDPR Concept of privacy Privacy concerns of cyberspace Constitutional framework of privacy Judicial interpretation of privacy in India	4
IV	**IP PROTECTION ISSUES IN CYBERSPACE:** Fundamental notions of copyright law Copyright issues in cyberspace Copyright infringement in digital environment-Software piracy, Linking, Framing, Caching, Meta Tagging, Legal protection of copyright in International Framework- WCT, WPPT, TRIPS. Indian legal protection of copyright in cyberspace & concept of DRM	4
V	**TRADEMARK ISSUES IN CYBERSPACE: Meaning**, Purpose and Kinds of Domain Name; Domain Name Vs Trademark, Domain Name Registration, ICANN, Domain Name dispute and Related Laws, Different Form of Domain in Cyberspace, Judicial Approach.	4

Text Books	1.	Apar Gupta, Commentary on Information Technology Act, 3rd Edition, Lexis Nexis, 2016.
	2.	N S Nappinai, Technology Laws Decoded, Lexis Nexis, 2017 Vakul Sharma, Information Technology Law and Practice, Universal Law Publishing,2017
	3.	Rodney D Ryder & Nikhil Naren, Internet Law-Regulating Cyberspace and emerging Technologies, Bloomsbury ,2020
E--Books	1.	https://store.lexisnexis.in/cyber-laws
Reference Books	1.	Pavan Duggal Cyber Law 3.0, Universal Law Publishing Company Private
	2.	Limited, 2014 Edition. Anirudh Rastogi, Cyber Law, Lexis Nexis, 2014.
Online TL Material	1.	https://youtu.be/KtuCsBlJXk8?feature=shared

Course Title: Web Cloud Computing Application										
Semester	III	Teaching Scheme				Evaluation Scheme				
Term	ODD					Theory			Practical	
Course Category	OE1	Th	Tu	Pr	Credits	TAE	CAE	ESE	Int	Ext
Course Code	BTCY2TT302	4 Hrs	NA	NA	4	10	15	50		
Teaching Mode	Offline									
Duration of ESE	3 Hrs	4 Hrs			Total	75				
						75				

Course Objectives	To study basics of cloud computing using force.com platform.
	To learn various aspects of sales force, like development, administration, Apex coding and reporting etc.
	To give students opportunities to build their carrier in cloud computing using Salesforce cloud Development platform.
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1: Understand fundamental concepts and technologies of cloud computing using Salesforce
	CO2: Apply Salesforce development skills to develop custom application on Salesforce cloud
	CO3: To handle responsibility of Salesforce Administrator
	CO4: To develop cloud application using visual force
	CO5: To implement custom business logic in Salesforce application using Apex.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcome	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2
CO1	--	--	3	--	--	--	--	--	--	--	--	--	--	--
CO2	--	--	--	3	--	--	--	--	--	--	--	--	--	--
CO3	--	--	3	--	--	--	--	--	--	--	--	--	--	--
CO4	--	--	--	--	3	--	--	--	--	--	--	--	--	--
CO5	--	2	--	--	--	--	--	--	--	--	--	--	--	--

Course Contents:

Unit	Contents	Hours
I	**Introduction:** Basics of Cloud computing using Salesforce, Salesforce - Home, Overview, Environment - Sales Cloud, Architecture, Service Cloud, Navigating Setup, Standard and Custom Objects, Master Detail, Schema Builder, Lookup Relationship	5
II	**Organization and User Setup, Security and Access:** Control Access Org, Control Access Objects, Control Access Fields, Control Access Records, Create a Role Hierarchy, Define Sharing Rules.	5
III	**Business logic & Process Automation:** Describe the function and use case of: Record type, Formula fields, Of roll-up summary fields, Validation rules, Approval process, Workflow, visual workflow and Lightning process builder: Working with Chatter, Chatter features, Chatter use cases Analyze data using reports and dashboards, Report type and dashboard, Identify the features available when creating a report	5
IV	**Visualforce:** Visualforce Pages, Variables & Formulas, Standard Controllers, Records, Fields &Tables, Using Forms, List Controllers, Static Resources. Action Function, Action Status, Action Support, Custom Controller and Extension	5
V	**Apex:** Introduction, Environment, data types, array, string, decision making, loops, collection, classes, objects, methods, DML, SOSL, SOQL	5

Text Books	1.	Salesforce.com For Dummies, 7th Edition by Liz Kho and Jon Paz
	2.	Salesforce Advanced Administrator Certification by Enrico Moru
EBooks	1.	https://trailhead.salesforce.com
	2.	https://success.salesforce.com
Reference Books	1.	Salesforce Handbook by Wes Nolte and Jeff Douglas
	2.	Learning Salesforce Lightning Application Development: buy Mohit Shrivastava.

SEMESTER - IV

<table>
<tr><td colspan="11">Course Title: DATABASE MANAGEMENT SYSTEM</td></tr>
<tr><td rowspan="2">Semester</td><td rowspan="2">IV</td><td colspan="4" rowspan="2">Teaching Scheme</td><td colspan="5">Evaluation scheme</td></tr>
<tr><td colspan="3">Theory</td><td colspan="2">Practical</td></tr>
<tr><td>Term</td><td>EVEN</td><td>Th</td><td>Tu</td><td>Pr</td><td>Credits</td><td>TAE</td><td>CAE</td><td>ESE</td><td>INT</td><td>EXT</td></tr>
<tr><td>Course Category</td><td>PCC4</td><td rowspan="2">3 Hrs.</td><td rowspan="2">.</td><td rowspan="2">2</td><td rowspan="2">4</td><td rowspan="2">10</td><td rowspan="2">15</td><td rowspan="2">50</td><td rowspan="2">25</td><td rowspan="2">25</td></tr>
<tr><td>Course Code</td><td>23BTCSL204CY/23BTCSP204CY</td></tr>
<tr><td>Teaching Mode</td><td>Offline</td><td colspan="3" rowspan="2">5 Hrs</td><td rowspan="2">Total</td><td colspan="3">75</td><td colspan="2">50</td></tr>
<tr><td>Duration of ESE</td><td>3 Hrs</td><td colspan="5">125</td></tr>
</table>

Course Objectives	This course introduces general idea of database management system, also gives idea to design databases using data modeling and design techniques.
	It is also aimed to developing skills to implement real life applications which involve database handling.
	This course also provide carrier opportunities in subject areas of designing, storage techniques and data handling and managing techniques
Course Outcomes	**CO1**: Analyze an information storage problem and derived an information model expression in the form of Entity relation diagram and design appropriate data model for it.
	CO2: Demonstrate SQL queries to perform CRUD (Create, Retrieve, Update, Delete) operations on database and perform inferential analysis of data model
	CO3: Identify features of database management systems and Relational database and understand functional dependencies and various normalization forms
	CO4: Perform basic transaction processing and management and ensure database security, integrity and concurrency control
	CO5: Analyze the management of structured and unstructured data management with recent tools and technologies

Department of Computer Science & Engineering (Cyber Security)

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes													
	PO1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO1 0	PO11	PO1 2	PSO 1	PSO 2
CO1	--	--	3	--	3	--	--	--	--	--		--	2	--
CO2	--	--	3	3	--	--	--	--	--	--		--	3	--
CO3	--	2	3	--	--	--	--	--	--	--	--	--	--	3
CO4	--	--	3	2	--	--	--	--	--	--	--	--	2	--
CO5	--	--	2	--	3	--	--	--	--	--	--	--	2	--

Course Contents:

Unit	Contents	Hours
I	Introduction to DBMS - DBMS Architecture, Data Models, E-R Diagram, Relational Database design:	6
II	SQL Concepts - Basics of SQL, DDL, DML, DCL, structure – creation, alteration, defining constraints, Functions - aggregate functions, Built-in functions –numeric, date, string functions, set operations, sub-queries, correlated sub-queries, Use of group by, having, order by, join and its types, Exist, Any, All, view and its types.	8
III	Functional Dependency (FD) – Basic concepts, closure of set of FD, closure of attribute set, Decomposition, Normalization – 1NF, 2NF, 3NF, BCNF, 4NF	5
IV	Transaction control commands – Commit, Rollback, Save point. Transaction Management: Transaction concepts, properties of transactions, serializability of transactions, Two- Phase Commit protocol, Deadlock, two-phase locking protocol. Cursors, Stored Procedures, Stored Function, Database Trigger, Database recovery.	7
V	Indexing and hashing, Query processing, Query Optimization, Data Mining, Advances in databases	4

Text Books	1.	Abraham Silberschatz, Henry F. Korth and S. Sudarshan, Database System Concepts 4th Ed, McGraw Hill, 2002.
	2.	Jeff Ullman, and Jennifer Widom, A First Course in Database systems, 2nd Ed.
E-Books	1.	https://ebooks.lpude.in/computer_application/mca/term_1/DCAP204_MANAGING_DATABASE_DCAP402_DATABASE_MANAGEMENT_SYSTEMS.pdf
Reference Books	1.	G. K. Gupta:" Database Management Systems", McGraw – Hill.
	2.	Regina Obe, Leo Hsu, PostgreSQL: Up and Running, 3rd Ed, O'Reilly Media 2017.
	3.	Kristina Chodorow, Shannon Bradshaw, MongoDB: The Definitive Guide, 3rd Ed, O'Reilly Media 2018.
	4.	RamezElmasri and ShamkantNavathe, Fundamentals of Database Systems 2nd Ed, Benjamin Cummings, 1994.
Online TL Material	1.	https://nptel.ac.in/courses/106/105/106105175/

Course Title: Computer Architecture and Operating System_NEP										
Semester	IV	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	EVEN	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PCC5	4	-	--	4	10	15	50	--	--
Course Code	23BTCYL204									
Teaching Mode	Offline	4			Total	75			-	
Duration of ESE	3 Hrs.					75				

Course Objectives	To provide essential understanding of different subsystems of modern computer system and design aspects these subsystems3
	Introduces general idea, structure and functions of operating system
	Making students aware of basic mechanisms used to handle processes, memory, Storage devices and files.
Course Outcomes	Upon successful completion of this course, student will be able to:
	CO1: Understand the basic components and design of a computer system
	CO2: Understand the concept of various memories and Pipelining technologies.
	CO3: Identify basic structure and purpose of operating system.
	CO4: Interpret the concepts of process, CPU scheduling algorithms and inter process communication.
	CO5: Schematize Deadlock, security mechanisms and different memory management techniques.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes														
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	1	2	3	--	--	--	--	--	--	--	--	--	-	-	1
CO2	--	2	3	--	--	--	--	--	--	--	--	--	2	2	1
CO3	--	3	3	--	--	--	--	--	--	--	--	--	2	--	-
CO4	--	3	2	--	--	--	--	--	--	--	--	--	3	3	1
CO5	--	3	2	--	--	--	--	--	--	--	--	--	--	3	-

Department of Computer Science & Engineering (Cyber Security)

Course Contents:

Unit	Contents	Hours
I	**Basic functional blocks of Computer:** Overview and history of computer architecture **Memory Architecture:** Memory hierarchy, Memory Chip Organization, Cache memory, Virtual memory, Parallel Bus Architectures, Internal Communication Methodologies, Serial Bus Architectures, Mass storage, Input and Output Devices, Segmentation, TLB, Page replacement algorithms, DMA	8
II	**Pipelining:** Basic concepts of pipelining, Arithmetic and Instruction Pipeline, throughput and speedup, pipeline hazards, Introduction, Logic Design Conventions, Building a Datapath- Pipelined Datapath and Control. Data Hazards: Forwarding versus Stalling, Control Hazards, Exceptions, Parallelism via Instructions, Software interrupt and exceptions.	8
III	**Operating System:** Evolution of OS, Types of OS, services provided by OS **Process & Its Scheduling:** Process concept, process control block, Types of scheduler, context switch, threads, multithreading model, goals of scheduling and different scheduling algorithms,	6
IV	**Process management and synchronization:** Concurrency conditions, Critical section problem, software and hardware solution, semaphores, conditional critical regions and monitors, classical inter process communication problems	6
V	**Deadlock**: definitions, Prevention, Avoidance, detection and Recovery, Goals of Protection, access matrix, Deadlock implementation **Memory Management & File systems:** File concept, Access methods space allocation strategies, disk arm scheduling strategies. Contiguous allocation, Relocation, Paging, Segmentation, Segmentation with paging, demand paging, Virtual Memory Concepts, page faults and instruction restart, page replacement algorithms	8

Text Books	1	Computer Organization and Architecture by Carl Hamacher 4th Edition
	2	Advance computer Architecture by Kai Hwang under Tata McGraw Hill Publications
	3	Introduction to Parallel Processing: Algorithms &Architectures, BehroozParhami in Springer Shop
	4	Operating System concepts – Silberchatz; Galvin, Addison Wesley, 6thEdn.
	5	Operating Systems: Internals and Design Principles -- William Stallings
Reference Books	1	Introduction to Parallel Processing by P. Ravi Prakash, M. Sasikumar, Dinesh Shikhare By PHI Publications
	2	Fundamentals of Parallel Processing by Jordan Harry, Alaghband Gita, PHI
	3	Operating Systems – S R Sathe, Macmillan Publishers, India, 2008
	4	Operating System –Milan Milenkovik, McGraw-Hill, 1987
	5	Operating Systems - 3 rd Edition by Gary Nutt, Pearson Education.
On line TL Material	1	NPTL https://nptel.ac.in/courses/106/105/106105163/
	2	https://nptel.ac.in/courses/106/108/106108101/

Course Title: MD2- Cyber Crimes and Investigation**_NEP_2020**										
Semester	IV	Teaching Scheme				Evaluation Scheme				
Term	EVEN					Theory			Practical	
Course Category	MD2	Th	Tu	Pr	Credits	TAE	CAE	ESE	Int	Ext
Course Code	**23BTCYL205**	2 Hrs	NA	NA	2	10	15	50	-	-
Teaching Mode	Offline									
Duration of ESE	3 Hrs	2 Hrs			Total	**75**			-	
						75				

Course Objectives	To extend the students' knowledge of Cyber Crimes & IT ACT
	To enhance their expertise in Cyber Crime Investigation and methodologies.
	To carry out real life cyber forensics assignments.
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1: Learning the basics of cyber-crime investigation
	CO2: Case studies of real-world cyber crimes
	CO3: Learning about IT act
	CO4: Indepth learning about data recovery tools, cyber forensics and ethics
	CO5: Analyzing investigation using various tools

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcome	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	**PSO 1**	**PSO 2**	**PSO 3**
CO1	2	2	3	--	2	--	--	--	--	1	--	--	3	3	3
CO2	2	--	--	3	--	2	2	--	2	--	--	2	2	2	3
CO3	2	2	3	--	--	--	--	--	--	--	2	--	2	1	2
CO4	--	--	2	2	3	--	--	2	2	--	--	--	1	2	1
CO5	3	2	--	--	--	--	--	--	--	--	--	--	1	2	2

Department of Computer Science & Engineering (Cyber Security)

Course Contents:

Unit	Contents	Hours
I	Introduction to Cyber Crime Investigation & Cyber Forensics Cyber Crime Investigation - Cyber Warfare, Terrorism & Social Networking - Cyber Forensics and Incident Handling - Case Study - Cyber Forensic Basics - Storage Fundamentals - File System Concepts	3
II	Investigating Real World Cyber Crimes Investigating Social Media Profile Impersonation cases - Phishing Cases - Data Theft Cases - Corporate Espionage Cases - Email Fraud Cases - Credit Card Fraud Cases - Cyber Pornography Cases - Denial of Service Attacks Cases - Cyber defamation Cases - Real Life Case Studies	4
III	IT ACT, Offenses and Penalties Offences under the Information and Technology Act 2000 - Penalty and adjudication - Punishments for contraventions under the Information Technology Act 2000 (Case Laws, Rules and recent judicial pronouncements to be discussed) - Limitations of Cyber Law	4
IV	Data Recovery Tools, Process, and Ethics & Cyber Forensics Investigation Gathering Evidence- Precautions, Preserving and safely handling original media for its admissibility - Document a Chain of Custody and its importance - Complete timeline analysis of computer files based on file creation - file modification and file access - Data Protection and Privacy. Introduction to Cyber Forensic Investigation – **Assignment: - Assignment should be a practical based on Tools**	4
V	Investigation Tools – eDiscovery - Digital Evidence Collection – Evidence Preservation - E-Mail Investigation - Encryption and Decryption methods - Search and Seizure of Computers – Work on open Source, Commercial tools and Cyber range **Assignment: - Assignment should be a practical based on Tools**	3

Text Books	1.	International domain name law: ICANN and the UDRP. Oxford: Hart Publishing by Lindsay D
	2.	. Investigating computer- related crime a handbook for corporate investigators. Boca Raton Stephenson P.R. & Gilbert K
Reference Books	1.	Incident response & computer forensics (2nd ed.) McGraw-Hill Companies by Prosise C. & Mandia K.
	2.	Cyber Law: The Law of the Internet and Information Technology. Pearson Education by Craig B 7. Incident response & com

Course Title: **Web Security-OE-II-NEP-2020**										
Semester	IV	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	EVEN	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	OE2	2		--	2	10	15	50	--	--
Course Code	23BTCYL206									
Teaching Mode	Offline	2			Total	75			--	
Duration of ESE	3 hrs					75				

Course Objectives	To reveal the underlying in web application.
	To identify and aid in fixing any security vulnerabilities during the web development process.
	To understand the security principles in developing a reliable web application.
Course Outcomes	**CO1:** Identify the vulnerabilities in the web applications.
	CO2: Identify the various types of threats and mitigation measures of web applications.
	CO3: Apply the security principles in developing a reliable web application.
	CO4: Use industry standard tools for web application security.
	CO5: Apply penetration testing to improve the security of web applications.

Mapping of Course Outcomes with Program Outcomes

Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	**PSO1**	**PSO2**	**PSO3**
CO1	3	3	2	2	2	1	1	1	1	1	1	2	3	2	1
CO2	3	3	2	2	2	2	1	1	1	1	1	2	2	3	2
CO3	3	2	2	3	3	2	2	2	2	1	1	2	2	2	2
CO4	3	2	2	2	2	2	1	2	2	2	2	2	3	3	2
CO5	3	3	3	2	2	2	2	2	1	2	3	3	2	2	2

Department of Computer Science & Engineering (Cyber Security)

Course Contents:

Unit	Content	Hours
1	Introduction history of web applications interface ad structure benefits and drawbacks of web applications, Web application Vs Cloud application Security Fundamentals: Input Validation - Attack Surface Reduction, Rules of Thumb- Classifying and Prioritizing Threads.	4
2	Understanding vulnerabilities in traditional client server application and web applications, client state manipulation, cookie based attacks, SQL injection, cross domain attack (XSS/XSRF/XSSI) http header injection, Proper encryption use in web application, Session vulnerabilities and testing, Cross-site request forgery. Case studies: Cookie Based Attacks, SQL Injection	5
3	Http request, http response, rendering and events, html image tags, image tag security, issue, java script on error, JavaScript timing, port scanning, remote scripting, running remote code, frame and iframe, domain relaxation. Case Studies: HTTP Request/Response, IFrame and Frame/Click Jacking	4
4	Secure website design: Architecture and Design Issues for Web Applications, Deployment Considerations Input Validation, Authentication, Authorization, Configuration Management, Sensitive Data, Session Management, Cryptography, Parameter Manipulation, Exception Management, Auditing and Logging, Design Guidelines, Forms and validity, Technical implementation Case Study: Web Architechure	4
5	Clickjacking - Java applet security - Single-sign-on solution and security, DNS rebinding - Flash security, IPv6 impact on web security	3

Reference Books:

1.	Web Application Security: Exploitation and Countermeasures for Modern Web Applications Paperback – Import, 13 March 2020 by Andrew Hoffman (Author)

Text Books:

1.	Sullivan, Bryan, and Vincent Liu. Web Application Security, A Beginner's Guide. McGraw Hill Professional, 2011.
	2. Stuttard, Dafydd, and Marcus Pinto. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. John Wiley Sons, 2011

E-Books:

1.	https://www.scribd.com/book/470612770/Penetration-Testing

Course Title: **Principles of Object Oriented Programming-NEP-2020**										
Semester	IV	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	Even	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	VSEC3	1	--	2	2	10	15	--	25	--
Course Code	23BTCYL207 23BTCYP207									
Teaching Mode	Offline	3 Hrs			Total	**25**			**25**	
Duration of ESE	3 Hrs					**50**				

Course Objectives	To introduce & understand the concepts of Object Oriented Programming.
	It is also aimed at developing skills to implement these concepts.
Course Outcomes	Upon successful completion of this course, students will be able to:
	CO1: Articulate the principles Object Oriented Programming concepts using the C++
	CO2: Applying various Datatypes and operators in program design.
	CO3: Able to Understand and Apply the concepts of Classes and objects in program
	CO4: Understanding the principles of data abstraction and Inheritance
	CO5: Analyse the various concept of OOP in a Java

Mapping of Course Outcomes with Program Outcomes & PSOs:

Course Outcomes	Program Outcomes														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1		3										3	2		
CO2			3									2	3		
CO3			2	3								2	3		
CO4				2								2	2		
CO5				3								2	2		

Course Contents:

Unit	Contents	Hours
I	**Introduction to Object Oriented Programming:** C++ overview. Basic C++ syntax, OOPParadigm, Basic Concepts of OOP, Benefits of OOP, Application of OOP.	2
II	**Tokens, Expression and controls Structures:** Data types, C++ tokens, Identifiers, Variables, Constants, Dynamic initialization of variables, Reference variables, expressions and Control Structures & loops	3
III	**Classes and Objects**: Introduction of Classes, Class Definition, Defining a Members, Objects, Access Control, Class Scope, Scope Resolution Operator, Inline functions, Memory Allocation for Objects, Arrays of Objects, Objects as Functions Arguments, Introduction to Constructors and Destructors.	4
IV	**Inheritance:** Single Inheritance, Multiple, Multilevel, Hierarchical Inheritance, Hybrid Inheritance, Friend Function, **Polymorphism:** Function overloading & operator overloading, virtual Function,	3
V	**Introduction to Java** Introduce the Java concept. Java Basics, Control Flow Statements, Object-Oriented Programming (OOP) Concepts	2

List of Experiments:

Sr. No.	Name of Experiments
1	Write a program to check whether the entered year is a leap year or not (a year is leap if it is divisible by 4 and divisible by 100 or 400.)
2	Write a program to find the largest of three numbers using ternary operators
3	Write a program to generate the Fibonacci series using Function.
4	Write a program to implement the concept of call by value & call by reference.
5	Write a Program in C++ to create a Number class. The class should contain a function to Increment and Decrement the number.
6	Write a program to implement the concept of Constructors.
7	Write a program to implement the Friend function
8	Write a program to create multilevel inheritance.
9	Write a Object oriented C++ Program to implement Virtual Function.
10	Write a program to implement the concept of Java programming

Text Books	1.	Object Oriented Programming in C++ -Robert Lafore, edition, Galgotia publications
	2.	The Complete Reference C++, Herbert Schildt, 4th Edition, TMH
	3	Programming with Java A Primer, E. Balaguruswamy Tata McGraw Hill Companies.
E-Books	1.	https://faculty.ksu.edu.sa/sites/default/files/ObjectOrientedProgramminginC4thEdition.pdf
	2.	https://faculty.ksu.edu.sa/sites/default/files/ObjectOrientedProgramminginC4thEdition.pdf
Reference Books	1.	Object oriented programming with C++, E Balagurusamy, 4th edition, TMH
	2.	Let's C++ by Y. Kanetkar, BPB publications
	3.	Robert Lafore - Object Oriented Programming in Microsoft C++ - Galgotia.

Course Title: Security in IoT_NEP-2020										
Semester	IV	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	Even	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	VSEC3	1	-	2	2	10	15	-	25	-
Course Code	23BTCYL208 23BTCYP208									
Teaching Mode	Offline	3 Hrs			Total	25			25	
Duration of ESE	3 Hrs					50				

Course Objectives	1. To learn about the security issues in IoT and cloud computing.
	2. To learn about the cryptography solutions and issues in IoT.
	3. To learn about the security measures taken in IoT and Cloud systems to improve security.
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1 - Understand the fundamental security issues in Internet of things.
	CO2 - Demonstrate different Frameworks and Hardware Architecture of IoT Device.
	CO3 - Analyze different IoT Protocols and Layer Functioning.
	CO4 - Protect and secure the network connecting IoT devices to back-end systems on the internet
	CO5 - Demonstrate different authentication mechanism such as digital certificates, biometrics, etc

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PS O3
CO1					3			3				3	3		
CO2					3			3				3	3		
CO3					3			3				3	3		
CO4					3			3				3	3		
CO5					3			3				3	3		

Course Contents:

Unit	Contents	Hours
I	**INTRODUCTION: SECURING THE INTERNET OF THINGS** Security Requirements in IoT Architecture, Security in Enabling Technologies, Security Concerns in IoT Applications. Insecure Access Control, Threats to Access Control, Privacy, and Availability, Attacks Specific to IoT. Vulnerabilities, Secrecy and Secret, Key Capacity.	4
II	**CRYPTOGRAPHIC FUNDAMENTALS FOR IOT** Cryptographic primitives and its role in IoT, Encryption and Decryption, Hashes, Digital Signatures, Random number generation, Cipher suites, Key management fundamentals, Cryptographic controls built into IoT messaging and communication protocols, IoT Node Authentication	4
III	**IDENTITY & ACCESS MANAGEMENT SOLUTIONS FOR IOT** Identity life-cycle, Authentication credentials, IoT IAM infrastructure, Authorization with Publish/Subscribe schemes, Access control	3
IV	**PRIVACY PRESERVATION FOR IOT** Privacy Preservation Data Dissemination, Privacy Preservation for IoT Used in Smart Building, Exploiting Mobility Social Features for Location Privacy Enhancement in Internet of Vehicles, Lightweight and Robust Schemes for Privacy Protection in Key Personal IoT Applications: Mobile WBSN and Participatory Sensing.	4
V	**CLOUD SECURITY FOR IOT** Cloud services and IoT, Offerings related to IoT from cloud service providers, Cloud IoT security controls, An enterprise IoT cloud security architecture, New directions in cloud enabled IoT computing	3

Books:

Text Books	1.	David Etter, " IoT Security: Practical guide book " Create Space, 1st Edition, 2016.
	2	FeiHU, "Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations", CRC Press, 2016
Reference Books	1.	Ollie Whitehouse, "Security of Things: An Implementers' Guide to Cyber-Security forInternet of Things Devices and Beyond", NCC Group, 2014
	2.	Drew Van Duren, Brian Russell, "Practical Internet of Things Security", Packt, 1st Edition, 2016.

Department of Computer Science & Engineering (Cyber Security)

Course Title: Aptitude and Employability Skills										
Semester	**IV**	**Teaching Scheme**				**Evaluation Scheme**				
						Theory			Practical	
Term	II	L	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	AEC2	1	-	2	2	10	15	-	25	--
Course Code	**23BTSHL231CY**									
Teaching Mode	Offline	3 HRS			**Total**	25			25	
Duration of ESE	3 Hrs					**50**				

Course Objectives	The Curriculum aims to equip students in order to apply quantitative reasoning and Mathematical analysis methodologies to understand and solve problems.
	To attain conceptual clarity to comprehend reasoning questions in a simple way and arrive at decisions at a logical manner.
	To introduce them with the current market scenarios and equip the students with the essential skills for employability
	To demonstrate self-sufficiency to be highly employable and assimilate how to prepare for personal interview
	To build self confidence facing any interview and consolidate job and career readiness
Course Outcomes	**CO1:** Students shall draw conclusions or make decisions based on analysis and critique of quantitative information. This leads them to effectively justify the conclusion and execute their plans.
	CO2: Students shall solve real life problems requiring interpretation and comparison of various probabilities to ascertain the best outcomes expected.
	CO3: Students shall exhibit their ability to set clear and realistic professional objective and enabling them to make well informed choices and commercially equipped according to market trends (Resume Building)
	CO4: Students shall be equipped on the application of organizing, planning and execution Skills (Personal Interview)

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes														
	PO 1	PO 2	PO3	PO4	PO5	PO6	PO7	PO8	PO 9	PO 10	PO 11	PO12	PSO 1	PSO 2	PSO 3
CO1	**3**	**3**													
CO2	**3**	**3**													
CO3				**2**							**2**	2			
CO4										**3**					
CO5									**3**	**3**					

Course Contents:

Unit	Contents
I	**Direction**: Introduction to direction nomenclature, Distance covered, Shortest possible distance by pythagoras theorem, Concept of Shadow -**Analogy**: All mathematical analogies -**Seating Arrangement**: Circular and Linear arrangement–**Syllogism**: Deductive reasoning, categorial syllogism, Some, All, few and Venn diagrams
II	**Data sufficiency**: Questions and statements -**Coding and Decoding**: Coding, Decoding & Patterns - **Number Series:** In place of alphabets the required number to be filled and addition and subtraction carried out accordingly – **Cryptarithmetic**: In place of alphabets the required number to be filled and addition and subtraction carried out accordingly
III	**Orientation - Researching Job and Company- Emerging Market Trends:** Experience sharing of Major Campus interviews, Skill Requirements, Current Market trends, Researching the Job and company
IV	**Personal and company commercial:** Guidelines for preparing a 30- 90 second self Introduction. Questions to think about in developing a commercial- Understand " What to avoid" in a commercial - **Self Selling Proficiency**: What to say and do, How to demonstrate commercial awareness in an interview, Post Interview activity, Telephone etiquette in a phone Interview **Resume Building:** Guidelines on framing resume and cover letter Checklist to ensure completeness, Sample resumes and cover letter references Basic Guidelines on Video Resume an its difference with conventional
V	**Personal Interview- Group Discussion**: Preparation tips on GD and Extempore: Dos' and Donts', Presentation on PI Preparation and FAQs -Role Plays/ Mock Interview with Technical Faculty and Mock Interview by Faculty **Assessment and feedback series:**

Text Books	1.	Aggarwal, R. S. (2010). A Modern Approach to Verbal & Non-Verbal Reasoning (Revised ed.). S. Chand Publishing. ISBN: 978-8121924986.
	2	Panikar, S., & Sharma, P. (2021). *Communication skills for budding professionals* (2nd ed.). Global Education Ltd
Reference Books	1.	Sharma, A., & Kumar, M. (2018). Quantitative Aptitude for Competitive Examinations. Pearson Education. ISBN: 978-9353061742.
	2.	Nair, M., & Mulay, T. (2024). *The golden book on employability: Get hired...stay hired* (1st ed.). Global Education Ltd.

Course Title: **Universal Human Values 2: Understanding Harmony**										
Semester	IV	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	EVEN	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	VEC2	2	--	--	2	10	15	50	--	--
Course Code	23BTSHL233CY									
Teaching Mode	Offline	2 HRS			Total	75			--	
Duration of ESE	3 Hrs.					75				

Course Objectives	Development of a holistic perspective based on self- exploration about themselves (human being), family, society and nature/existence
	Understanding (or developing clarity) of the harmony in the human being, family, society and nature/existence
	Strengthening of self-reflection and development of commitment and courage to act.
Course Outcomes	1. Students are expected to become more aware of themselves.
	2. Students are expected to become more aware of their surroundings (family, society, nature).
	3. Students should become more responsible in life, and in handling problems with sustainable solutions, while keeping human relationships and human nature in mind.
	4. Students would have better critical ability, they would also become sensitive to their commitment towards what they have understood (human values, human relationship and human society).
	5. Students would be able to apply what they have learnt to their own self in different day-to-day settings in real life.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes														
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1						**2**		**3**	**1**			**2**			
CO2			**3**			**2**		**2**		**2**		**2**			
CO3			**3**			**3**	**3**	**2**							
CO4			**2**			**2**	**2**	**2**							
CO5			**1**			**1**	**1**	**2**				**3**			

Course Contents:

Unit	Contents	Hours
I	**Course Introduction - Need, Basic Guidelines, Content and Process for Value Education:** Purpose and motivation for the course, Self-Exploration, Continuous Happiness and Prosperity, Right understanding relationship and physical facility, Understanding happiness and prosperity correctly, Method to fulfill the above human aspirations.	8
II	**Understanding Harmony in the Human Being - Harmony in Myself!** Understanding human being as a co-existence of the sentient 'I' and the material 'Body', Understanding the needs of Self ('I') and 'Body', Understanding the Body as an instrument of 'I', Understanding the characteristics and activities of 'I' and harmony in 'I', Understanding the harmony of I with the Body.	8
III	**Understanding Harmony in the Family and Society- Harmony in Human-Human Relationship** Understanding values in human-human relationship, Understanding the meaning of Trust, Understanding the meaning of Respect, Understanding the harmony in the society, Visualizing a universal harmonious order in society.	8
IV	**Understanding Harmony in the Nature and Existence - Whole existence as Coexistence** Understanding the harmony in the Nature, Interconnectedness and mutual fulfillment among the four orders of nature, Understanding Existence as Co-existence, Holistic perception of harmony.	8

Text Book	1.	Human values and Professonal Ethics by R R Gaur,R Sangal,G P Bagaria,Excel Books,New Delhi,2010
Reference Books	1.	Jeevan Vidya: Ek Parichaya,A Nagaraj, JeevanVidya Prakashan, Amarkantak,1999
	2.	Human Values, A.N.Tripathi, New Age Intl. Publishers, New Delhi 2004.
	3.	The story of my experiments with truth-by Mohandas Karamchand Gandhi
	4	Small is beautiful-E. F Schumacher
	5	Slow is beautiful-Cecile Andrews

SEMESTER – V

Course Title: Fundamentals of Cryptography										
Semester	V	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	ODD	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PCC6	3	1	-	4	10	15	50	-	-
Course Code	23BTCYL301									
Teaching Mode	Offline	4 Hrs			Total	75			-	
Duration of ESE	3:00 Hr					75				

Course Objectives	Understanding of the basic concepts of Cryptography
	To understand the techniques of Classical Cryptosystems
	To understand concepts of Symmetric cryptography
	To understand concepts of Asymmetric cryptography
	To Provide students with a comprehensive overview of Message Authentication Code and Hash Functions
Course Outcomes	CO1: To elaborate the role of cryptography & its fundamentals
	CO2: To apply various cryptography techniques
	CO3: To apply concepts of Symmetric cryptography
	CO4: To apply concepts of Asymmetric cryptography
	CO5: TO analyze MAC and Hash Codes

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes													
	PO 1	PO 2	PO3	PO4	PO 5	PO 6	PO 7	PO 8	PO 9	PO1 0	PO11	PO12	PSO1	PSO 2
CO1	**2**	**2**	**3**										**3**	
CO2		**2**												**2**
CO3		**3**											**1**	
CO4			**3**	**3**										**2**
CO5	**3**			**3**										

Course Contents:

Unit	Contents	Hours
I	**Introduction to Cryptography:** Introduction to Cryptography, History of Cryptography, Shannon's Description of a Conventional Cryptosystem, Statistical Description of a Plaintext Source, Problems, Attacks, services, mechanisms, security attacks, security services, a model for internetwork security, encryption model, steganography.	8
II	**Classical Cryptosystems:** Caesar, Simple Substitution, Caesar Cipher, Playfair , Simple Substitution Cryptanalysis by The Method of a Probable Word.VigenèreCryptosystem, Kasiski's Method, Transpositions, Rail Fence The One-Time Pad Transposition, Rotor Machines. INTRODUCTION TO NUMBER THEORY: Prime Numbers, Fermat's and Euler's Theorem, Testing for Primality, The Chinese Remainder Theorem, Discrete logarithms,	8
III	PUBLIC KEY CRYPTOGRAPHY AND RSA: Principles Public key crypto Systems, Diffie Hellman Key Exchange, the RSA algorithm, Key Management, Elliptic Curve Arithmetic, Elliptic Curve Cryptography. MESSAGE AUTHENTICATION AND HASH FUNCTIONS: Authentication Requirement, Authentication Function, Message Authentication Code, Hash Function, Security of Hash Function and MACs. HASH AND MAC ALGORITHM: Secure Hash Algorithm, Whirlpool, HMAC, CMAC. DIGITAL SIGNATURE: Digital Signature, Authentication Protocol, Digital Signature Standard.	8
IV	AUTHENTICATION APPLICATION: Kerberos, X.509 Authentication Service, Public Key Infrastructure. Dictionary Attack, Biometric System EMAIL SECURITY: Pretty Good Privacy (PGP) and S/MIME. IP SECURITY: Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management.	8
V	WEB SECURITY: Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET), Intruders, Viruses and related threats. FIREWALL: Firewall Design principles, Trusted Systems. Malicious Logic: Types of Malicious Logic: Virus, Worm, Trojan Horse, Zombies, Denial of Service Attacks, Intrusion, Intruders and their types, Intrusion Detection System	8

Text Books	1.	a) . "Cryptography and Network Security: Principles and Practice" by William Stallings (1st ed. 1995, latest ed. 2020).
On line TL Material	1.	1. nptel.ac.in/courses/106105031 (IIT K) 2. https://nptel.ac.in/courses/106105031/39 3. https://nptel.ac.in/courses/106106129 4. https://onlinecourses.nptel.ac.in/noc18_cs24 5. https://onlinecourses.nptel.ac.in/noc22_cs03/preview 6. https://archive.nptel.ac.in/courses/106/106/106106221/

Course Title: Cyber Laws and Ethics										
Semester	V	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	ODD	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PCC7	3Hrs.	-	-	3	10	15	50	-	-
Course Code	23BTCYL302									
Teaching Mode	Offline	3Hrs			Total	75				
Duration of ESE	3Hrs.									

Course Objectives	1. Gain foundational knowledge of cyber law and its application within the Indian legal system
	2. Understand the integration of the Bhartiya Nyaya Sanhita and its influence on cyber law
	3. Familiarize with cybercrime sections and punishments under the current Indian framework
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1: Understanding Cyber Law and its Impact on the Indian Legal System
	CO2: Identification of Cybercrimes and Legal Consequences
	CO3: Identify Critical Analysis of Cyber Ethics in Digital Environments
	CO4: Understand Application of Intellectual Property Laws in Cyberspace
	CO5: Understand Comprehension of E-Governance, Digital Contracts, and Cyber security Frameworks

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes													
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**
CO1								2				2	1	
CO2								3				2	1	
CO3								3				2	3	
CO4								2				3		1
CO5								1				2		1

Course Contents:

Unit	Contents	Hours
I	**Cyber Ethics and Ethical Issues in Cyberspace:** **1. Importance of Cyber Ethics:** Definition of **Cyber Ethics**: The moral and ethical principles governing online behaviour, Ethical concerns in cyberspace: data privacy, intellectual property, and online content regulation. **2. Ethical Challenges in Emerging Technologies:** Exploring the ethical challenges posed by AI, data analysis in digital transactions, Digital Privacy: Ethical implications of surveillance, tracking, and data harvesting. **3. Ethical Codes and Regulations:** The role of the Indian Computer Emergency Response Team (CERT-In) in promoting cyber ethics. BNS Ethical Considerations	8Hrs.
II	**Introduction to Cyber Laws and the Bhartiya Nyaya Sanhita:** **1. Overview of Cyber Law in India:** Introduction to Cyber Law and its significance in the Indian legal system, Bhartiya Nyaya Sanhita (BNS): How the BNS impacts legal frameworks for cyberspace, Key cyber laws in India, including the Information Technology Act, 2000, and its amendments. **2. Legal Provisions under IT Act and Punishments:** Detailed examination of Section 66, Section 67, Section 43A, and other BNS sections, Punishments: Legal consequences of cybercrimes under the BNS framework (e.g., hacking, cyber-stalking, identity theft). **3. Overview of Indian Cyber Jurisprudence:** Evolution of cyber jurisprudence in India with notable **case studies.**	8Hrs.
III	**Cybercrime and Punishments:** **1. Types of Cybercrimes: Hacking and Cyber-terrorism**: Legal definitions, case studies, and punishments under Section 66 of the IT Act and related sections of BNS, Cyberbullying: Legal responses and ethical challenges, Identity Theft and Phishing. **2. Cybercrime Investigation and Law Enforcement:** Role of law enforcement in investigating cybercrimes, Tools and technologies used for cybercrime prevention, **Case studies**	7Hrs.

IV	**Intellectual Property Rights in Cyberspace:** **1. Copyright and Trademarks in the Digital World: Copyright Protection**: Legal protections for digital content, software, and online media under Indian copyright law, **Trademarks**: Legal issues related to domain names, cybersquatting, and the use of trademarks in cyberspace. **2. Software Piracy and Patent Issues:** Legal consequences of software piracy and digital piracy under the **Bhartiya Nyaya Sanhita**, Patent law issues in the context of digital inventions and technology. **3. Intellectual Property Disputes in Cyberspace:** Case studies	8Hrs.
V	**E-Governance, Digital Contracts, and Legal Frameworks:** **1. Legal Recognition of Electronic Records: E-Governance in India**: Legal framework for the recognition of electronic documents and records under the **Indian Evidence Act, 1872**. **2. Cybersecurity and the Role of Certifying Authorities:** The role of **Certifying Authorities** (CAs) in securing digital records and authentication, India's cybersecurity initiatives and the establishment of the **Cyber Appellate Tribunal.** **Case studies.**	8Hrs.

Text Books	1.	"Cyber Law and E-Commerce" by S. S. Gulshan A comprehensive guide on cyber laws, including case studies and legal principles applied in India
	2.	"Information Technology Act 2000: Law and Practice" by Dr. Gaurav Agrawal A detailed study of the IT Act, with sections on amendments, challenges, and judicial interpretations
	3.	"Bhartiya Nyaya Sanhita" (Updated 2024 Edition) The latest provisions, amendments, and punishments under the Bhartiya Nyaya Sanhita, specifically addressing issues in cyber law and ethics.
Reference Books	1.	"Cyber Law in India" by P.K. Agarwal In-depth analysis of cyber law in India, including its evolution, challenges, and judicial pronouncements.
	2.	"Ethics of Artificial Intelligence and Robotics" by Vincent C. Müller Discusses ethical issues surrounding emerging technologies such as AI and its implications on cyber law.
	3.	"Principles of Cyber Security and Digital Law" by Gurpreet KaurFocuses on the interplay between cybersecurity, digital laws, and ethical principles in cyberspace
On line TL Material	1.	**Primer on New Criminal Laws (NCL)** **By Dr. Neeraj Tiwari | National Law University** **https://onlinecourses.swayam2.ac.in/cec25_lw03/preview**
	2	**Introduction to Cyber Law** **By Alison** **https://alison.com/course/introduction-to-cyber-law**

Course Title: **Introduction to Penetration Testing**										
Semester	V	Teaching Scheme				Evaluation Scheme				
						Theory				
Term	ODD	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PCC8	2 Hrs	NA	2 Hrs	3	10	15	50	25	-
Course Code	23BTCYL303/ 23BTCYP303									
Teaching Mode	Offline	4 Hrs			Total	75			25	
Duration of ESE	3 Hrs					100				

Course Objectives	To understand how intruders escalate privileges.
	To understand Intrusion Detection, Policy Creation, Social Engineering, Buffer Overflows and different types of Attacks and their protection mechanisms
	To learn about penetration testing.
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1: Understand the concept of penetration testing.
	CO2: To apply technique of reconnaissance.
	CO3: Evaluate exploitation and elaborate the technology.
	CO4: Understanding post exploitation maintaining access.
	CO5: Apply and execute the penetration test.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	**Program Outcomes and Program Specific Outcomes**														
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	**3**	**3**					**1**	**2**	**2**	**2**		**2**		**2**	**1**
CO2	**3**	**3**					**1**	**2**	**1**	**1**		**3**		**2**	**2**
CO3	**3**	**3**	**3**	**2**	**2**	**2**	**1**	**3**	**1**	**2**	**2**	**2**	**2**	**3**	**3**
CO4	**3**	**3**	**3**	**3**	**3**	**2**	**1**	**2**	**2**	**1**	**2**	**2**	**2**	**2**	**3**
CO5	**3**	**3**	**3**	**3**	**3**	**2**	**1**	**1**	**3**	**3**	**3**	**3**	**3**	**3**	**3**

Course Contents:

Unit	Contents	Hours
I	**INTRODUCTION TO PENETRATION TESTING:** Introduction - Terminologies - Categories of Penetration Testing - Phases of Penetration Test -Penetration Testing Reports - Information Gathering Techniques - Active, Passive and Sources of Information Gathering - Approaches and Tools- Traceroutes, Neotrace, Whatweb, Netcraft, Xcode Exploit Scanner and NSlookup. Host discovery - Scanning for open ports and services.	4
II	**RECONNAISSANCE:** Reconnaissance: HTTrack: Website Copier- Google Directives: Practicing Your Google-Fu. - The Harvester: Discovering and Leveraging E-mail Addresses, Fierce and Other Tools to Extract Information from DNS. -Extracting Information from E-mail Servers. -Threat Agent: Attack of the Drones. -Sifting through the Intel to Finding Attackable Targets.	4
III	**EXPLOITATION:** Medusa: Gaining Access to Remote Services - Metasploit: Hacking Hugh Jackman Style - John the Ripper: King of the Password Crackers - Password Resetting: The Building and the Wrecking Ball - Wireshark: Sniffing Network Traffic - Wireshark: Sniffing Network Traffic. - Armitage: Breaking Out the M-60.	4
IV	**POST EXPLOITATION AND MAINTAINING ACCESS:** Netcat: The Swiss Army Knife - Cryptcat: Netcat's Cryptic Cousin - Rootkits - Hacker Defender: It is Not What You Think - Detecting and Defending Against Rootkits - Meterpreter: The Hammer that Turns Everything into a Nail	4
V	**APPLYING THE PENETRATION TEST** Writing the Penetration Testing Report - You Do Not Have to Go Home but You Cannot Stay Here - Where Do I Go from Here? - Wrap Up -The Circle of Life	4

Text Books	1.	Weidman, Georgia. Penetration testing: a hands-on introduction to hacking /Georgia Weidman. IN 2014.
E--Books	1.	https://www.scribd.com/book/470612770/Penetration-Testing
Reference Books	1.	Sean -Philip oriyano "penetration testing essentials", Released December 2016 Publisher(s): Sybex ISBN: 9781119235309
	2.	Patrick Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy", Syngress Basics Series – Elsevier, August 4, 2011.
	3.	Philip L. Wylie "The Pentester Blueprint" SBN-139781119684305 Publisher:Wiley
Online TL Material	1.	https://www.youtube.com/watch?v=q-ZrX41cIOA

Department of Computer Science & Engineering (Cyber Security)

PRACTICAL LIST

Course Name: Introduction to Penetration Testing
Course Outcome:

CO1: Understand the concept of penetration testing.
CO2: To apply technique of reconnaissance.
CO3: Evaluate exploitation and elaborate the technology.
CO4: Understanding post exploitation maintaining access.
CO5: Apply and execute the penetration test.

Practical No.	List of Practical	COs
01	**Introduction to Penetration Testing**: To identify and install Virtual machines and Operating Systems used in Penetration Testing	CO1
02	**Monitoring Network Traffic**: To analyze and capture network traffic to identify patterns, detect anomalies and assess overall network performance and security.	CO1
03	**Host & Services Discovery using Nmap**: To identify active hosts and the services they are running within a network using Nmap, enabling a comprehensive understanding of the network environment.	CO2
04	**Vulnerability Scanning using OpenVAS**: To perform a systematic assessment of networked systems using OpenVAS to identify potential vulnerabilities that could be exploited by attackers.	CO2
05	**Internal Penetration Testing:** To perform a thorough internal penetration test that systematically assesses the security of the organization's network infrastructure by mapping network resources, scanning for vulnerabilities, exploiting known weaknesses and demonstrating attack techniques, including credential sniffing and poisoning attacks, in order to identify and mitigate potential	CO3
06	**External Penetration Testing:** To conduct a comprehensive external penetration test aimed at evaluating the security of the organization's external infrastructure by assessing vulnerabilities, mapping the network topology, gathering IP and domain registry information, and examining the implementation of IPv6, ultimately identifying potential entry points and recommending measures to strengthen defenses against external threats.	CO3
07	**Different Types of Vulnerability Scanning:** To explore and compare various vulnerability scanning techniques and tools, assessing their effectiveness in identifying and prioritizing security risks.	CO4

08	**Vulnerability Scanning with Nessus:** To utilize Nessus for comprehensive vulnerability scanning, identifying security weaknesses in systems and providing recommendations for remediation.	CO4
09	**Web Application Assessment with Nikto Suite:** To evaluate web applications for security vulnerabilities using Nikto, identifying issues such as misconfigurations and common vulnerabilities in web applications.	CO5
10	**Web Application Assessment with Burp Suite:** To evaluate web applications for security vulnerabilities using Burp, identifying issues such as misconfigurations and common vulnerabilities in web applications.	CO5
Practical Beyond Syllabus (Open Ended)		
11	Install and Implement various commands Wireshark on Linux	CO3
12	Case study on: PTES Framework (Penetration Testing Methodologies and Standards)	CO5

Course Title: Ethical Hacking-PE1										
Semester	V	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	ODD	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PEC1	3	-	2	4	10	15	50	25	
Course Code	23BTCYL304/ 23BTCTP304									
Teaching Mode	Offline	5 Hrs			Total	75			25	
Duration of ESE	3 Hrs					100				

Course Objectives	1. To understand how intruders escalate privileges.
	2 To understand Intrusion Detection, Policy Creation, Social Engineering, Buffer Overflows and different types of Attacks and their protection mechanisms
	3. To learn about ethical laws and tests
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1- Understand the legal and ethical requirements related to ethical hacking.
	CO2 – Identifying how to access an environment using foot-printing.
	CO3 - Apply Data Security in various environment.
	CO4 - Creating Network Protection System & Hacking Web Servers.
	CO5 - Analyze the tools for conducting ethical hacking.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes												Program Specific Outcomes		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	2	2	2			2		2	1	2			2	3	2
CO2			2								2		2	2	2
CO3	2			3			2		2				1	2	
CO4				2					2		2		1	2	
CO5	2				2								2	2	3

Department of Computer Science & Engineering (Cyber Security)

Course Contents:

Unit	Contents	Hours
I	**INTRODUCTION TO ETHICAL HACKING:** Ethical Hacking Definition, difference between hacking and ethical hacking. Vulnerability, Attack Vector. Five stages of hacking: Reconnaissance (Survey), Probing, Actual attack, maintaining presence, Covering attack tracks, Introduction to OWASP top 10 vulnerabilities.	6
II	**SCANNING AND SYSTEM HACKING: Port Scanning, Network Scanning, Vulnerability Scanning, NMAP Scanning tool, OS Fingerprinting** **System Hacking: Password cracking techniques, Key loggers, Escalating privileges, URL Hiding Files, Sniffers & SQL Injection: Active and passive sniffing, ARP Poisoning, Session Hijacking, DNS Spoofing, Conduct SQL Injection attack, Counter measures. Study of open source scanning tools.**	7
III	**DATA SECURITY: Physical Security –** Attacks and Protection, Steganography – Methods, Attacks and Measures, Cryptography – Methods and Types of Attacks, Wireless Hacking, Windows Hacking, Linux Hacking.	5
IV	**NETWORK PROTECTION SYSTEM & HACKING WEB SERVERS:** Routers, Firewall & Honeypots, IDS & IPS, Web Filtering, Vulnerability, Penetration Testing, Session Hijacking, Web Server, SQL Injection, Cross Site Scripting, Exploit Writing, Buffer Overflow, Reverse Engineering, Email Hacking, Incident Handling & Response, Bluetooth Hacking, Mobiles Phone Hacking.	7
V	HACKING ENVIRONMENT DAMN VULNERABLE WEB APPLICATION (DVWA) Installation and configuration of DVWA environment. Virtual box installation, Installation of Kali Linux within virtual box. Kali Linux penetration testing and ethical hacking tools. What is TOR? How can you use it to protect your anonymity online? Social Engineering: Phases of an attack, Common targets, Common sources of information. Web Servers and applications: Common attacks and flaws, Current tools.	7

Text Books	1.	Michael T. Simpson, Kent Backman, James E. "Corley, Hands-On Ethical Hacking and Network Defense", Second Edition, CENGAGE Learning, 2010.
Reference Books		**Steven DeFino, Barry Kaufman, Nick Valenteen, "Official Certified Ethical Hacker Review Guide", CENGAGE Learning, 2009-11-01.**
	2.	Patrick Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy", Syngress Basics Series – Elsevier, August 4, 2011

Practical No.	Experiment Name
1	Study and Demonstration of the Five Stages of Hacking
2	Introduction to OWASP Top 10 vulnerabilities
3	To perform port scanning on a target system to identify open ports and services using Nmap, and understand the role of port scanning in ethical hacking and network reconnaissance.
4	To perform network scanning using tools like **Nmap** and **Netdiscover** to identify live hosts, open ports, and network services within a target network.
5	To perform vulnerability scanning on a target system or web application using tools like **Nikto** and **Nessus**, and analyze discovered vulnerabilities.
6	To study and implement basic cryptographic techniques
7	To study and apply **steganography techniques** to hide and extract information within digital media (images, audio files, etc.) using common tools.
8	To understand and implement a honeypot in a network for detecting and analyzing unauthorized access attempts.
9	To understand and exploit Cross-Site Scripting (XSS) vulnerabilities in a web Application
10	To understand the concept of Session Hijacking

Course Title: AI for IoT Applications										
Semester	V	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	ODD	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PE-I	3	-	2	4	10	15	50	25	-
Course Code	23BTCYL305/ 23BTCYP305									
Teaching Mode	Offline	5 Hrs			Total	75			25	
Duration of ESE	3 Hrs					100				

Course Objectives	1. To equip students with an understanding of how Artificial Intelligence (AI) and Machine Learning (ML) can be integrated into Internet of Things (IoT) applications
	2 To explore the principles, methods, and tools for implementing AI-based solutions in IoT environments.
	3. The students will be proficient in applying AI techniques to enhance the functionality of IoT systems
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1- Grasp the role of AI in enhancing IoT functionality.
	CO2 - Apply machine learning algorithms to process IoT data
	CO3 - Apply AI-based data analytics to real-time IoT systems.
	CO4 - Understand and implement deep learning techniques in IoT applications.
	CO5 - Understand the ethical and regulatory challenges of integrating AI into IoT applications.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes													
	PO 1	**PO 2**	**PO 3**	**PO 4**	**PO 5**	**PO 6**	**PO 7**	**PO 8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO 1**	**PSO 2**
CO1		2											2	
CO2			2										2	
CO3				3									1	
CO4				2									1	
CO5					2									2

Course Contents:

Unit	Contents	Hours
I	**Introduction to IoT and AI** Overview of Internet of Things (IoT): Architecture, Components, and Applications, Introduction to Artificial Intelligence (AI): History, Scope, and AI vs ML, Role of AI in IoT: Data Analysis, Decision Making, and Predictive Models, IoT-AI Integration: Challenges and Opportunities	6
II	Machine Learning Techniques for IoT Data Supervised and Unsupervised Learning Algorithms, Regression, Classification, Clustering, and Dimensionality Reduction, Data Preprocessing for IoT Sensor Data,	6
III	**AI-based Data Analytics and Predictive Modelling** Data Analytics: From Data Acquisition to Visualization, Time Series Forecasting for IoT: Techniques and Applications, Predictive Maintenance in IoT Systems, Anomaly Detection in IoT Data Streams	8
IV	**Deep Learning and Edge AI** Applying Deep Learning to IoT: Object Recognition, Sensor Fusion, Convolutional Neural Networks (CNN) for Image Processing in IoT, Recurrent Neural Networks (RNN) for IoT Time Series Data, Edge AI and Edge Computing in IoT Systems, Lightweight machine learning Models eg. MobileNet, SqueezeNet, TinyML Models.	8
V	Security, Privacy, and Ethical Considerations in AI for IoT Security and Privacy Issues in IoT Systems, Securing AI in IoT: Approaches for Data Encryption and Authentication, Ethical Implications of AI in IoT: Bias, Transparency, and Accountability, Blockchain for IoT Security, AI for Threat Detection in IoT Networks, Regulations and Standards for AI-enabled IoT Systems **Case study absed on IOT Application**	8

Text Books	1.	**Artificial Intelligence: A Modern Approach** -by Russell/Norvig (Author) Publisher-Pearson Education Edition-4, Publication Date-31 May 2022
	2	**Confluence of AI and IoT : Marriage Made in Heaven** -by Vinay Solanki (Author) Publisher-Notion Press, Publication Date-30 December 2022
Reference Books	1.	**AI for Everyone: A Beginner's Handbook for Artificial Intelligence (AI) - by Saptarsi Goswami (Author) Publisher-Pearson Education-Publication Date-23 May 2024**
	2.	**The Today and Future of WSN, AI, and IOT** by Dr.Chandrakant (Author), Dr Suresh (Author) ,ISBN-13-978-9389845167, Publication Date-1 January 2020

Sr.no	Name of Experiments
1	Assemble a basic IoT device using a microcontroller (e.g., Raspberry Pi or Arduino) and connect it to the cloud.
2	Implement a basic AI decision tree for an IoT-based home automation system.
3	Use Scikit-learn or TensorFlow to implement regression and classification for IoT sensor data.
4	Create visualizations of IoT sensor data and predictions using Python libraries like Matplotlib.
5	Develop a simple predictive maintenance model using time series forecasting for an industrial IoT scenario.
6	Design a small-scale smart healthcare monitoring system leveraging predictive analytics.
7	Apply convolutional neural networks (CNNs) for IoT-based image recognition (e.g., detecting objects using a smart camera).
8	Use RNNs for time series data, such as predicting weather patterns from IoT sensors.
9	OPEN ENDED Practical 1
10	OPEN ENDED Practical 2

Course Title: Computer Security										
Semester	V	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	ODD	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	MDM3	3	-	2	4	10	15	50	25	-
Course Code	23BTCYL307/ 23BTCYP307									
Teaching Mode	Offline	5 Hrs			Total	75			25	
Duration of ESE	3 Hr					100				

Course Objectives	Understanding of the basic concepts of Computer Security
	To understand the techniques of Networks security
	To understand concepts of Web security
	To understand concepts of Server Security
	To Provide students with a comprehensive overview of Disaster Recovery and Fault Tolerance.
Course Outcomes	**CO1:** Apply basic concepts of Computer Security
	CO2: Analyze the techniques of Networks security
	CO3: Remember the concepts of Web security
	CO4: Apply the concepts of Server Security
	CO5: Evaluate the concepts in Disaster Recovery and Fault Tolerance.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes														
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	**3**	**2**	**0**	**1**	**2**	**1**	**0**	**2**	**0**	**1**	**0**	**2**	**3**	**2**	**1**
CO2	**2**	**3**	**2**	**2**	**3**	**1**	**0**	**2**	**0**	**1**	**1**	**2**	**1**	**3**	**1**
CO3	**2**	**2**	**1**	**1**	**2**	**1**	**0**	**1**	**0**	**1**	**0**	**2**	**3**	**2**	**1**
CO4	**3**	**2**	**2**	**2**	**3**	**1**	**0**	**2**	**0**	**1**	**1**	**2**	**2**	**3**	**2**
CO5	**2**	**3**	**2**	**3**	**2**	**1**	**0**	**2**	**1**	**2**	**2**	**3**	**2**	**2**	**3**

Course Contents:

Unit	Contents	Hours
I	**Introduction to computer security** Overview of Computer Security Concepts and Foundations Threats, Attacks, and Assets. **Computer Security Technology and Principles** User Identification and Authentication Access Control Database and Cloud Security Malicious Software Denial-of-Service Attacks Intrusion Detection **Firewalls:** Types of Firewalls, design principles, trusted systems, Honeypots.	6
II	**Networks security practice:** E-mail security: pretty Good privacy, S/MIME. **IP security:** overview, architecture, authentication header, encapsulating security payload, combining security associations, key management. Intrusion Prevention Systems (IPS), Secure N/2 Design and Architecture	6
III	**Web security:** Requirements, secure electronic transaction, networks management security. System Security: Intruders, viruses and worms, Web Browser Security - Email Security Firewall VPN - Transport Layer Security (TLS) Handshake Protocol Alert Message Protocol Chan	10
IV	**Server Security:** Server Roles and Security Server Roles and Baselines - Securing Network Infrastructure Servers DNS. DHCP, WINS, Remote Access Servers, NAT servers, RTO (Recovery Time Objective) and RPO (Recovery Point Objective), BCB and BIA. Domain Controllers – Securing File and Print Servers -Securing Application Servers	6
V	**Disaster Recovery and Fault Tolerance** Planning for the Worst -Creating a Backup Strategy -Designing for Fault Tolerance Antivirus **Privacy rules:** Access, data backup and type of data backup, test security systems and processes. Mobile/Cloud security issues and challenges in futuristic web security applications. Load balancers, Byte Streams Checksums - Custom Check-sums - Cryptographic Hashes Advanced Signatures - Fuzzy Hashing - Graph-Based Hashes for Executable Files	10

Text Books	1.	1 Computer System Security: Basic Concepts and Solved Exercises (Computer and Communiaction Sciences) Hardcover – Illustrated, 13 July 2007by Gildas Avoine (Author), Philippe Oechslin (Author), & 1 More 2. Computer System and Network Security Edited By Eric A. Fisch, Gregory B. White ISBN 9781138583085Published August 10, 1995 by CRC Press310 PagesCopyright Year 1996
E--Books	1.	https://www.researchgate.net/publication/220117871_Security_of_Computer_Systems_and_Networks_Book_Preview

Department of Computer Science & Engineering (Cyber Security)

Practical No.	Topic to be covered
1	**Practical No 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	**Practical No 2** Study the steps to protect a Microsoft Word Document of different version with different operating system
3	**Practical No 3** Study the steps to remove Passwords from Microsoft Word
4	**Practical No 4** Study various methods of protecting and securing databases.
5	**Practical No 5** Study "How to make strong passwords" and "passwords cracking techniques".
6	**Practical No 6** Study of different wireless network components and features of any one of the Mobile Security Apps.
7	**Practical No 7** Study of the features of firewall in providing network security and to set Firewall Security in windows.
8	**Practical No 8** Steps to ensure Security of any one web browser (Mozilla Firefox/Google Chrome)
9	**Practical No 9** Study of different types of vulnerabilities for hacking a websites / Web Applications.
10	**Practical No 10** Analysis the Security Vulnerabilities of E-commerce services.
11	**Practical No 11** Open Ended Practical: Analysis the Security Vulnerabilities of E-mail services.

Department of Computer Science & Engineering (Cyber Security)

Course Title: Principles of Cryptography										
Semester	V	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	ODD	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	OE3	2	-	-	2	10	15	50	-	-
Course Code	23BTCYL308									
Teaching Mode	Offline	2 Hrs			Total	75			-	
Duration of ESE	3 Hr					75				

Course Objectives	To understand the techniques of Classical Cryptosystems
	To understand concepts of Symmetric cryptography
	To understand concepts of Asymmetric cryptography
	To Provide students with a comprehensive overview of Message Authentication Code and Hash Functions
Course Outcomes	CO1: Elaborate the role of cryptography & its fundamentals
	CO2: Apply various cryptography techniques
	CO3: Understand concepts of Symmetric cryptography
	CO4: Understand concepts of Asymmetric cryptography
	CO5: Analyze MAC and Hash algorithms

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes													
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2
CO1	**2**	**2**	**3**										**3**	
CO2		**2**												**2**
CO3		**3**											**1**	
CO4			**3**	**3**										**3**
CO5	**3**			**3**										

Department of Computer Science & Engineering (Cyber Security)

Course Contents:

Unit	Contents	Hours
I	**Introduction to Cryptography:** Introduction to, Terminology, History of Cryptography, Shannon's Description of a Conventional Cryptosystem, Statistical Description of a Plaintext Source, Problems, Attacks, services, mechanisms, security attacks, security services.	4
II	**Classical Cryptosystems:** Caesar, Simple Substitution, Caesar Cipher, Playfair,Simple Substitution Cryptanalysis by The Method of a Probable Word. VigenèreCryptosystem ,Kasiski's Method, Transpositions, Rail Fence The One-Time Pad Transposition.	4
III	**Introduction to Symmetric cryptography:** Symmetric cryptography, algorithms under symmetric cryptography.Block Ciphers Some General Principles Some Block Cipher ModesCodebook Mode Cipher Block Chaining Cipher Feedback Mode DES DES, Triple DES and IDEA .	5
IV	**Introduction to Asymmetric cryptography:** Asymmetric cryptography, algorithms under asymmetric cryptography, placement of encryption function, traffic confidentiality, key distribution, Public key cryptography, Chinese remainder theorem, discrete logarithms.	4
V	**Message Authentication and Hash Functions** Authentication requirements, functions, codes, security of hash function & MACs. Hash & MAC algorithms. Digital signatures & authentication protocols.	3

Text Books	1.	a) Cryptography and networks security principles & practice by William Stallings (Pearson Education prentice Hall b) FUNDAMENTALS OF CRYPTOLOGY KLUWER ACADEMIC PUBLISHERS By Henk C.A. van Tilborg Eindhoven University of Technology The Netherlands
E--Books	1.	Cryptography and networks security principles & practice by William Stallings (Pearson Education prentice Hall

Course Title: Research Methodology										
Semester	V	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	Odd	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	RM	-.	-	4 Hrs	2	-	-	-	25	-
Course Code	23BTSHP301									
Teaching Mode	Offline	4Hrs			Total				25	
Duration of ESE	-					25				

Course Objectives	1. To understand the role of research methodology in Engineering.
	2. To understand data collection methods and basic instrumentation.
	3. To learn various statistical tools for data analysis.
	4. To develop the ability to apply statistical tools and techniques.
	5. To provide knowledge on sampling design.
Course Outcomes	CO1: Understand the role of research methodology in Engineering
	CO2: Apply appropriate techniques for data collection
	CO3: Analyze collected data using editing, classification, coding, and quantitative methods
	CO4: Apply statistical methods for data analysis
	CO5: Evaluate sampling designs and apply suitable sampling techniques

Mapping of Course Outcomes with Program Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1		3		3											
CO2		3		3	1										
CO3		3	3	3	2										
CO4				3	1										
CO5		3		3							2				

Department of Computer Science & Engineering (Cyber Security)

Course Contents:

Unit	Contents	Hours
I	**Introduction to Research**: Definition of research, Characteristics of research, Types of research- Descriptive vs. Analytical, Applied vs. Fundamental, Quantitative vs. Qualitative, Conceptual vs. Empirical, Overview of research methodology in various areas, Introduction to problem solving, basic research terminology such as proof, hypothesis, lemma etc., Role of Information and Communication Technology(ICT) in research.	6
II	**Data Collection:** Primary Data: Meaning, Importance & limitations, Observation , Questionnaire, Interview, Interview Scheduled Social Survey, Case Study Secondary Data: Meaning, Importance& limitations. Sources Secondary Data.	6
III	**Data Analysis And Use Of Quantitative Method**: Editing, Classification and Coding. Categorization, Tabulation, Tables, Graphs, Illustrations. Use of quantitative method in research.	6
IV	**Data Analysis And Use Of Statistical Method:** Statistical Techniques: Measures of Central tendency, Dispersion, Skewness, Kurtosis & Moments, Correlation, Regression. Theory of Attributes & Association, chi squareTest & Distribution.	6
V	**Sampling Design:** Census and sample survey, Characteristics of good sample design, Implications of sample design, Sampling Techniques, Probability or random sampling, Non-probability sampling	6

Text Books	1	Ranjit Kumar, "Research Methodology: A Step by Step Guide for Beginners", SAGE Publications Ltd., 2011.
	2	C.R. Kothari ,"Research Methodology: Methods and Trends", New Age International,2004
	3	Gupta S.C, Fundamentals of Statistics, Himalaya Publication House, Bombay Rajaram V. (1996),
E--Books	1	Wayoc C. Booth : The Craft of Research
	2	David Willinson : Research Tools Kits : A Complete Guide to Practitioner Research
Reference Books	1	Wayne Goddard, Stuart Melville, "Research Methodology: An Introduction" JUTA and Company Ltd, 2004.
on line TL Material	1	http:// www.shodhaganga.inflibnet.ac.in
	2	http:// www.inflibnet.ac.in.
	3	http:// www.zotero.org

Sr. No.	Name of Experiments / Mini Projects/ Case Studies (Any 8)
1	Report writing explaining importance of research. (CO1)
2	To collect data using two different methods. (CO2)
3	Performing literature review, identifying gaps (CO3)
4	Design simple sampling method for survey (CO3)
5	Raw data coding and classification (CO3)
6	Formulation of hypothesis based on collected data (CO3)
7	Using bar graphs, pie charts for interpreting findings (CO4)
8	Project proposal that includes problem identification. (CO5)
9	Ethical consideration in research methodology. (CO5)

Department of Computer Science & Engineering (Cyber Security)

SEMESTER-VI

Course Title: **Principles of Algorithm Design**										
Semester	VI	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	Even	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PCC9	3 Hrs.	-	2 hrs.	4	10	15	50	25	25
Course Code	23BTCYL310/23BTCYP310									
Teaching Mode	Offline	5 Hrs.			Total	75			50	
Duration of ESE	3 Hrs.					125				

Course Objectives	This course introduces students the general idea of analysis and design of Algorithms while making them aware of basic methods of algorithm analysis and design.
	It is also aimed at developing skills to solve real life applications which involve algorithm development
	The course also provides career opportunities in analysis, design and optimization technique in algorithms
Course Outcomes	CO1: Recall basic concepts of algorithm in analysis and Design of algorithms.
	CO2: Examine Recurrence relations, solutions of recurrence of searching sorting methods
	CO3: Apply Greedy methods used for analysis and Design of Algorithm
	CO4: Analyze Dynamic Programming concepts in designing algorithm
	CO5: Evaluate advanced techniques and tools available for algorithm analysis and development

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO 1	PSO 2
CO1	--	3	--	--	--	--	--	--	--	--	--	--	2	--
CO2	--	--	3	--	--	--	--	--	--	--	--	--	1	--
CO3	--	--	--	3	--	--	--	--	--	--	--	--	2	--
CO4	--	--	3	--	--	--	--	--	--	--	--	--	2	--
CO5	--	--	3	--	--	--	--	--	--	--	--	--	2	--

Course Contents:

Unit	Contents	Hours
I	**Unit – I: Mathematical foundations & Asymptotic notations** summation of arithmetic and geometric series, n, n2, Complexity calculation of various standard functions, Principles of designing algorithms, Asymptotic notations of analysis of algorithms, analyzing control structures, worst case and average case analysis, Iterative Algorithm analysis.	9
II	**Unit -II Divide & Conquer Method:** Recurrence relations, solutions of recurrence relations using technique of Characteristic equation and generating functions Divide and conquer basic strategy, matrix operation, Strassens matrix multiplication, binary search, quick sort, merge sort.	8
III	**Unit – III: Greedy Method** Greedy method – basic strategy, application to job sequencing with deadlines problem, minimum cost spanning trees, single source shortest path, Huffman Coding, Prim's Algorithm, Kruskal's Algorithm, Dijkstra's Algorithm	8
IV	**Unit IV: Dynamic Programming** Dynamic Programming basic strategy, multistage graphs, all pairs shortest path, single source shortest paths, optimal binary search trees, traveling salesman, Knapsack, sum of subset problems	8
V	**Unit V: Traversal and Search Techniques** Basic Traversal and Search Techniques, breadth first search and depth first Search, Backtracking basic strategy, 8-Queen's problem, graph coloring, Hamiltonian cycles, NP-HARD AND NP-COMPLETE PROBLEMS: Basic concepts, non-deterministic algorithms, NP-hard and NP-complete classes.	9

Textbooks	1.	Thomas H. Cormenet. al. "Introduction to Algorithms", Prentice Hall of India.
	2.	Design & Analysis of Computer Algorithms by Aho, Horowitz, Sahani, Rajsekharam, Pearson education
Reference Books	1.	"Computer Algorithms", Galgotia Publications Pvt. Ltd. Brassard, Bratley, "Fundamentals of Algorithms", Prentice Hall
	2.	Computer Algorithms: Introduction to Design and analysis, 3rd Edition, By Sara Baase & A. V. Gelder Pearson Education.
On-line TL Material	1.	NPTEL course on Design and Analysis of Algorithms**:** https://www.class-central.com/course/nptel-design-and-analysis-of-algorithms-3984

Department of Computer Science & Engineering (Cyber Security)

PRACTICAL LIST

Sr.	Title of Practical	Hrs.	Relevance
1	To Implement and analyze time complexity of Searching Algorithm.	2	CO1
2	To Implement and analyze time complexity of Sorting Algorithm.	2	CO1
3	To Implement and analyze time complexity of algorithm using Divide and Conquer Technique.	2	CO2
4	To Implement and analyze time complexity of Greedy Algorithm.	2	CO2
5	Implement Prim's algorithm using an adjacency matrix or list.	**2**	**CO3**
6	**Case Study:** Conference Room Booking System A company has multiple meeting requests. Design a system that selects the maximum number of meetings without time	**2**	**CO3**
7	To implement and analyze time complexity of Single source shortest path Algorithm.	2	CO4
8	To implement and analyze time complexity of All pair shortest path Algorithm.	2	CO4
9	To implement and analyze time complexity of Graph Traversing Algorithm.	2	CO5
10	Open-Source Practical	2	CO5

Course Title: **Data Analytics**										
Semester	VI	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	Even	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PCC10	3	-	2	4	10	15	50	25	25
Course Code	23BTCYL312/23BTCYP312									
Teaching Mode	Offline	5 Hrs			Total	75			50	
Duration of ESE	3 Hrs.					125				

Course Objectives	To perform descriptive statistics on the given dataset
	To perform inferential statistics on the given dataset
	Apply linear regression and logistic regression and perform data visualization on the given dataset.
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1: Generate the dataset and perform Descriptive Statistics
	CO2: Evaluate the dataset and perform an Inferential Statistics
	CO3: Apply regression Analysis on the given dataset
	CO4: Create an interactive data visualization
	CO5: Recite the various learning techniques to derive case study

Department of Computer Science & Engineering (Cyber Security)

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes		Program Outcomes and Program Specific Outcomes													
	PO 1	PO 2	PO3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO1	PS O 2	PS O 3
CO1	**3**			**2**		**2**				**2**			**2**		**1**
CO2	**3**							**2**					**2**		**2**
CO3			**3**				**2**		**3**		**2**		**3**	**1**	
CO4			**3**						**2**		**1**			**3**	**2**
CO5					**3**					**2**				**2**	**2**

Course Contents:

Unit	Contents	Hours
I	Data Analytics: Introduction to Analytics, Introduction to Tools and Environment, Application of Modeling in Business, Databases and Types of Data and variables, Data Modeling Techniques, Missing Imputations etc. Need for Business Modeling.	8
II	Descriptive statistics, data preparation. Exploratory Data Analysis data summarization, data distribution. Visualizing numerical data - graphing systems, measures of central tendency and dispersion – correlation - transforming data - exploring categorical variables.	8
III	Regression: linear regression simple linear regression, multiple & Polynomial regression, Sparse model. Supervised Learning: First step, learning curves, training validation and test. Learning models generalities, support vector machines, decision trees and random forest.	9
IV	Unsupervised learning, clustering, similarity and distances, quality measures of clustering, case study.	5
V	Classification and Prediction Issues Regarding Classification and Prediction, Classification by Decision Tree Induction, Bayesian Classification, and Classification Methods, Prediction, Classifier Accuracy.	8

Text Books	1.	Data Analytics: The Complete Beginner's Guide: the Black Book,Byron Francis, CreateSpace Independent Publishing Platform, 2016
	2.	Gupta S. C., & Kapoor V. K., Fundamental of Mathematical Statistics, Sultan Chand & Sons, 2018.
	3.	Teetor P, R cookbook: Proven recipes for data analysis, statistics, and graphics, O' Reilly Media Inc., 2011.
E--Books	1.	Fundamentals of Mathematical Statistics, Gupta SC, Kapoor V.K.. Publisher: Sultan Chand & Sons. Publishing Year: 2020. http://dcpehvpm.org/EContent/Stat/FUNDAMENTAL%20OF%20MATHEMATICAL%20STATISTICSS%20C%20GUPTA%20&%20V%20K%20KAPOOR.pdf
Reference Books	1.	Joel Grus, Data Science from Scratch First Principles with Python, O'Reilly Media, 2016

Department of Computer Science & Engineering (Cyber Security)

List of Practical

Sr. No.	Name of Experiments
1	Loading dataset and visualizing data
2	Producing descriptive statistics measures
3	Demonstrate handling of missing data
4	Demonstrate Scatter Plot
5	Demonstrate Histogram Plot
6	Demonstrate Linear Regression for a given dataset
7	Demonstrate Multiple Linear Regression for a given dataset
8	Demonstrate Logistic Regression for a given dataset
9	Demonstrate Clustering for a given dataset
10	Demonstrate random Forest method for a given dataset
Open Ended Experiments / New Experiments	
1	Demonstrate Classification for a given dataset
2	Demonstration of data analysis on virtual Lab
1.	https://www.iiitmk.ac.in/DAVirtalLab/#work

Course Title: E-II_IOT using Robotics_NEP										
Semester	VI	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	EVEN	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PEC2	3	-	2	4	10	15	50	25	--
Course Code	23BTCYL317/23BTCYP317									
Teaching Mode	Offline	5			Total	75			-	
Duration of ESE	3 Hrs.					75				

Course Objectives	To introduce the fundamental concepts of IoT and robotics
	To develop understanding of sensors, actuators, microcontrollers, and embedded systems
	To provide hands-on experience in programming, interfacing, and deploying IoT-enabled robots.
Course Outcomes	Upon successful completion of this course, student will be able to:
	CO1: Explain the fundamental concepts, architecture, and components of IoT and robotics.
	CO2: Identify and interface sensors, actuators, microcontrollers, and communication modules used in IoT-enabled robotic systems.
	CO3: Design IoT-based robotic applications for data acquisition, monitoring, and control.
	CO4: Develop and program embedded systems (Arduino, Raspberry Pi, etc.) for IoT-robotics integration.
	CO5: Analyze real-time data, networking protocols, and security issues in IoT-robotic environments.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO2	PSO3
CO1	1	2	3	--	--	--	--	--	--	--	--	--	-	-	1
CO2	--	2	3	--	--	--	--	--	--	--	--	--	2	2	1
CO3	--	3	3	--	--	--	--	--	--	--	--	--	2	--	-
CO4	--	3	2	--	--	--	--	--	--	--	--	--	3	3	1
CO5	--	3	2	--	--	--	--	--	--	--	--	--	--	3	-

Course Contents:

Unit	Contents	Hours
I	**Introduction to IoT and Robotics** Overview of Internet of Things (IoT): Definition, characteristics, applications Basics of Robotics: Types of robots, components of a robotic system, IoT Architecture: Perception, Network, Middleware, Application layers, Embedded Systems for IoT and Robotics,Communication technologies: Wi-Fi, Bluetooth, ZigBee, RFID, LoRa ,Role of IoT in modern robotics and automation	8
II	**Sensors, Actuators, and Interfacing** Sensors used in robotics: Proximity, IR, Ultrasonic, Temperature, Motion, IMU Actuators: DC motors, Servo motors, Stepper motors, Relay modules, Sensor Integration with microcontrollers, Motor driver circuits: L293D, L298N ,Data acquisition and signal processing basics, Practical Interfacing with Arduino/Raspberry Pi	8
III	**Microcontrollers and IoT Platforms** Arduino: Architecture, digital & analog I/O, timers, interrupts, Raspberry Pi: Architecture, GPIO programming, Python-based control, ESP8266/ESP32: Wi-Fi-enabled microcontrollers, IoT communication protocols: MQTT, HTTP, CoAP Cloud Platforms: ThingsSpeak, Blynk, AWS IoT, Google Firebase,Building IoT-based robotic control systems	8
IV	**Robotics Control & Automation** Robot control algorithms: Line following, obstacle avoidance, path planning, Autonomous robot design concepts, Interfacing sensors/actuators for robotic decision-making ,Real-time data monitoring and control, Wireless robotic control using IoT apps, Integration of robotics with cloud dashboards ,Case studies: Smart car, home automation robot, surveillance robot	8
V	**Security, OT Systems, Real-Time, Edge Computing & Tools** Operational Technology (OT) & Cyber-Physical Security Introduction to OT systems: PLC, SCADA, DCS, ICS,Difference between IT vs OT networks,OT hardware in robotics & automation,Communication protocols used in OT: Modbus, OPC-UA, Profibus, BACnet,Definition of real-time systems in IoT-robotics ,Hard vs Soft real-time systems ,Example applications: autonomous robots, AGVs, industrial robots, drones ,What is edge computing & why it is needed ,Reduce latency for real-time robot control,Edge devices: Raspberry Pi, Jetson Nano, ESP32,IoT security basics: Vulnerabilities, authentication, encryption ,Secure communication for IoT-enabled robots , Real-time data analytics and remote diagnostics .Security Tools for IoT, OT & Robotics: Wireshark,Nmap,Kali Linux Tools,Metasploit.	8

Text Books	1	Internet of Things: Architecture and Design Principles **Author:** *Raj Kamal*
	2	Robotics: Control, Sensing, Vision, and Intelligence **Author:** *K. S. Fu, R. C. Gonzalez, C. S. G. Lee*
	3	Getting Started with Arduino **Authors:** *Massimo Banzi & Michael Shiloh*
	4	Learning Robotics Using Python **Author:** *Lentin Joseph*
	5	Designing the Internet of Things **Authors:** *Adrian McEwen & Hakim Cassimally*
Reference Books	1	Internet of Things: Robotic and Drone Technology **Author:** *C. S. R. Prabhu*
	2	Embedded Robotics: Mobile Robot Design and Applications with Embedded Systems ***Author:*** Thomas Bräunl
	3	Introduction to Embedded Systems and Robotics: A Practical Guide **Author:** *N. Yadav, M. Sharma, D. Shukla*
online TL Material	1	NPTEL – Introduction to Internet of Things
	2	Coursera – IoT Specialization (University of California, Irvine)

Department of Computer Science & Engineering (Cyber Security)

EXP NO.	LIST OF EXPERIMENT	Mapping with CO
	Mini Project: IoT Surveillance Robot **Objective:** Integrate sensors, camera, wireless control, telemetry, and cloud dashboard into a working prototype.	
1	Study IoT Architecture, Wi-Fi connectivity using ESP32/NodeMCU,Robotics, Real-time image streaming	CO-1
2	To design and integrate an **IoT-controlled mobile robot** for surveillance purposes.	CO-1
3	Requirements (Hardware & Software) like Arduino/NodeMCU/ESP32, Motor driver (L293D/L298N), DC motors or robotic chassis, ESP32-CAM or USB camera, PIR sensor / Ultrasonic sensor, IoT platform: Blynk / Firebase / MQTT Dashboard, Mobile app or Web dashboard	CO-2
4	To interface sensors (camera, PIR, obstacle sensors) with a microcontroller.	CO-2
5	To Assemble the robotic chassis and connect motors to the motor driver. Interface ESP32/NodeMCU with sensors and camera module.	CO-3
6	To implement **real-time remote monitoring** using IoT platforms (Blynk/Thingspeak/Firebase).	CO-4
7	Configure IoT app dashboard for robot control and live monitoring.	CO-4
8	To evaluate system performance and demonstrate applications in security automation.	CO-5

Course Title: Web Application Security										
Semester	VI	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	EVEN	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PEC2	3	-	2	4	10	15	50	25	-
Course Code	23BTCYL315/ 23BTCYP315									
Teaching Mode	Offline	5Hrs			Total	75			25	
Duration of ESE	3 Hr					100				

Course Objectives	1. To reveal the underlying in web application.
	2. To identify and aid in fixing any security vulnerabilities during the web development Process
	3. To understand the security principles in developing a reliable web application.
Course Outcomes	CO1. Identify the vulnerabilities in the web applications.
	CO2. Identify the various types of threats and mitigation measures of web applications.
	CO3. Apply the security principles in developing a reliable web application.
	CO4 Use industry standard tools for web application security.
	CO5. Apply penetration testing to improve the security of web applications

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1	2	3	1	2	3	1	0	2	1	1	0	2	3	2	1
CO2	2	3	2	2	3	2	1	2	1	1	0	2	3	3	1
CO3	2	2	3	1	3	1	1	2	1	2	1	2	2	3	1
CO4	1	2	2	2	3	1	0	1	1	1	1	2	2	3	1
CO5	2	3	2	3	3	2	1	2	1	2	1	3	3	3	2

Course Contents:

Unit	Contents	Hours
I	**Overview of Web Applications Security Fundamentals** Introduction history of web applications interface ad structure benefits and drawbacks of web applications Web application Vs Cloud application Security Fundamentals: Input Validation - Attack Surface Reduction Rules of Thumb- Classi- fying and Prioritizing Threads. Origin Policy - Exceptions to the Same-Origin Policy - Cross-Site Scripting and Cross-Site Request Forgery - Reflected XSS - HTML Injection	8
II	**Web Application Vulnerabilities** Understanding vulnerabilities in traditional client server application and web applications, client state manipulation, cookie based attacks, SQL injection, cross domain attack (XSS/XSRF/XSSI) http header injection. SSL vulnerabilities and testing - Proper encryption use in web application- Session vulnerabilities and testing - Cross-site request forgery.	8
III	**Web Application Mitigations** Http request, http response, rendering and events, html image tags, image tag security, issue, java script on error, JavaScript timing, port scanning, remote scripting, running remote code, frame and iframe, browser sandbox, policy goals, same origin policy, library import, domain relaxation	8
IV	**Secure Website Design** Secure website design: Architecture and Design Issues for Web Applications, Deployment Considerations Input Validation, Authentication, Authorization, Configuration Management, Sensitive Data, Session Management, Cryptography, Parameter Manipulation, Exception Management, Auditing and Logging, Design Guidelines, Forms and validity, Technical implementation	8
V	**Cutting Edge Web Application Security** Clickjacking - DNS rebinding - Flash security - Java applet security - Single-sign-on solution and security - IPv6 impact on web security	8

Text Books	1.	Sullivan, Bryan, and Vincent Liu. Web Application Security, A Beginner's Guide. McGraw Hill Profe ssional, 2011. 2. Stuttard, Dafydd, and Marcus Pinto. The Web Application Hacker's Handbook: Finding and **Exploiting Security Flaws. John Wiley Sons, 2011**
E--Books	1.	
Reference Books	1.	Web Application Security: Exploitation and Countermeasures for Modern Web Applications Paperback – Import, 13 March 2020 by Andrew Hoffman (Author)

Sr No	Name of Experiment	CO
1	Study and Analysis of Web Application Architecture and Security Fundamentals	CO1
2	Demonstration of Input Validation and Detection of HTML Injection /Reflected XSS	CO1
3	Study of Client-Side State Management and Cookie-Based Attacks	CO2
4	Identification and Testing of SQL Injection & HTTP Header Injection Vulnerabilities	CO2
5	Analysis of the Security Vulnerabilities of E-commerce services	CO3
6	Analysis of the security vulnerabilities of E-Mail Application	CO3
7	Make a Detailed Report on Network Security Threats covering Structured, Unstructured, Internal and External Threats	CO4
8	Configuring IPSec VPN Tunnel Mode using Packet Tracer	CO5
9	Open Ended	--
10	Open Ended	--

Department of Computer Science & Engineering (Cyber Security)

Course Title: Digital Forensics (E -III)										
Semester	VI	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term		Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PEC3	4	-	-	4	10	15	50	-	-
Course Code	23BTCYL321									
Teaching Mode	Offline	4 Hrs			Total	75			-	
Duration of ESE	3 Hrs					75				

Course Objectives	To understand underlying principles and many of the techniques associated with the digital forensic practices and cyber-crime.
	To develop an excellent understanding of current cyber security issues (Computer Security Incident) and analyze the ways that exploits in securities.
	To investigate attacks, IDS. Technical exploits and router attacks and "Trap and Trace" computer networks.
	To learn the importance of evidence handling and storage for various devices.
	To apply digital forensic knowledge to use computer forensic tools and investigation report writing.
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1: Analyze threats in order to protect or defend it in cyberspace from cyber-attacks.
	CO2: Develop appropriate security solutions against cyber attacks.
	CO3: Select different types of tools for various phases of forensics investigation
	CO4: Create reports as per standards of digital forensics.
	CO5: Understand he method to generate legal evidence and supporting investigation reports and will also be able to use various digital forensic tools.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes													
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1		**1**		**3**				**2**		**2**		**3**	**3**	
CO2			**2**	**1**	**3**							**3**		**2**
CO3		**1**		**2**	**3**							**3**	**1**	
CO4		**3**									**1**	**2**		
CO5				**1**	**3**							**2**		

Course Contents:

Unit	Contents	Hours
I	**Fundamentals of Digital Forensics** Foundations of Digital Forensic: Digital evidence, Awareness, Principles of Digital Forensic,Challenging aspects of digital evidence, Cyber trail. Language of Computer Crime Investigation:Role of Computers in crime, Cybercrime law, offenses, jurisdiction. Traffic analysis, Fraud, IT Act	6
II	**Computer Forensic** Digital Evidence: Digital evidence in courtroom: Duty of experts, Admissibility, Locard's exchange principle, Types of Evidence, The Rules of Evidence, Volatile Evidence, Evidence collection and Archiving, Methods of Collection, Collection Steps, Controlling Contamination: The Chain of Custody. Processing Computer Crime: Introduction to Crime Scenes, Seizing and storing digital evidence at scene, Documenting the Scene and the Evidence, Dealing with Live Systems and Dead Systems, Using Hashing to Verify the Integrity of Evidence.	7
III	**Data Acquisition and Data Recovery** Data acquisition- Understanding storage formats and digital evidence, determining the best acquisition method, acquisition tools, validating data acquisitions, performing RAID data acquisitions, remote network acquisition tools, other forensics acquisitions tools Data Recovery: Data Backup and Recovery, The Role of Backup in Data Recovery, The Data-Recovery Solution Hiding and Recovering Hidden Data, Data Handling tools, ISO 27001.	6
IV	**Mobile device Forensic and Email Forensics** Mobile Device Forensics, Types of evidence on mobile device, Handling mobile device as a sources of evidence, Forensic prevention of mobile devices, Forensic examination , analysis of mobile devices, Forensic acquisition , examination of SIM cards (Architecture, Data Storage, Files, Mobile Operating System), Investigative reconstruction using mobile devices, Mobile Forensics and its challenges, Email Forensics: EMail Header Analysis, Function & Forensics, Chat and Social Networking Evidence. Case study	7
V	**Forensic Investigation Report and Forensic Tools:** Goals of Report, Layout of an Investigative Report, Guidelines for Writing a Report, sample for writing a Forensic report. Computer Forensic Tools: need and types of computer forensic tools, task performed by computer forensic tools. Study of open source Tools like SFIT, Autopsy etc. to acquire, search, analyze and store digital evidence. Case study	7

Text Books	1. Digital Evidence; Computer Crime – Forensic science, Computers; The Internet', Eoghan Casey, 3rd edition 2. 'Computer Forensics Computer Crime scene investigation', 2nd edition, Johm R. Vacca 3. Cyber Law Simplified, Vivek Sood 4. Basics of Digital Forensics, Second edition – John Sammons
Reference Books	4. Computer Forensics Investigating Network Intrusions & Cybercrime', EC–Council press, Cengage Learning 5. Guide to Computer Forensics & Investigations, 4th edition, Bill Nelson, Amelia Phillips & Christopher Steuart, Cengage Learning 6. 'Guide to Integrating Forensic Techniques into Incident Response', NIST, Karen Kent, Suzanne Chevalier Tim Grance, Hung Dang

Course Title: Privacy and Security in IOT/OT										
Semester	VII	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term		Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PEC3	4	-	-	4	10	15	50	-	-
Course Code	23BTCYL323									
Teaching Mode	Offline	4			Total	75			-	
Duration of ESE	3 Hr					75				

Course Objectives	1. Understand the foundational concepts of IoT security and privacy
	2. Investigate the privacy challenges posed by IoT data collection
	3. Apply security protocols and cryptographic techniques to IoT systems
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1: Understand the IoT Vulnerabilities and authentication issues
	CO2: Analyze IoT-specific privacy issues and identify potential security threats
	CO3: Apply cryptographic and authentication techniques to secure IoT devices.
	CO4: Develop IoT security frameworks and solutions, including privacy-preserving protocols.
	CO5: Evaluate real-world IoT security scenarios and design secure IoT systems

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1	**2**	**2**	**0**	**1**	**2**	**1**	**0**	**2**	**0**	**1**	**0**	**2**	**3**	**2**	**1**
CO2	**2**	**3**	**2**	**2**	**3**	**1**	**0**	**2**	**0**	**1**	**1**	**2**	**2**	**3**	**1**
CO3	**2**	**2**	**2**	**1**	**2**	**1**	**0**	**1**	**0**	**1**	**0**	**2**	**3**	**2**	**1**
CO4	**3**	**2**	**2**	**3**	**3**	**1**	**0**	**2**	**0**	**1**	**1**	**2**	**2**	**3**	**3**
CO5	**2**	**3**	**2**	**3**	**2**	**1**	**0**	**2**	**1**	**2**	**3**	**3**	**2**	**2**	**3**

Course Contents:

Unit	Contents	Hours
I	**Introduction to IoT and its Security Challenges:** Overview of IoT: Definition, architecture, and applications. Components of IoT Systems: Sensors, actuators, gateways, and cloud platforms, Security Challenges in IoT: Device security, data privacy, network security, authentication, and authorization issues. IoT Vulnerabilities: Security and privacy threats in IoT devices and communication protocols. IoT Security Standards: Overview of current IoT security standards and best practices (e.g., IEEE 802.15.4, ZigBee, 6LoWPAN, etc.).	8
II	**Privacy in IoT Systems:** Privacy Issues in IoT: The role of IoT in data collection, personal data, and privacy risks, Data Sensitivity in IoT: Types of data (location, health, personal activities) and their sensitivity, Privacy Regulations: GDPR, CCPA, and other privacy laws impacting IoT data, Indian Law,Digital DPDP,Privacy Preservation Techniques: Data anonymization, differential privacy, and privacy-preserving protocols, Case Studies: Real-world IoT privacy violations and the lessons learned.	7
III	**IoT Security Mechanisms:** IoT Security Requirements: Confidentiality, integrity, availability, authentication, non-repudiation, Cryptographic Techniques: Symmetric and asymmetric encryption, hashing, and digital signatures, Authentication and Authorization: Multi-factor authentication (MFA), public key infrastructure (PKI), OAuth, and access control models, Secure Communication Protocols: TLS/SSL, MQTT, CoAP, and secure channels in IoT, Intrusion Detection and Prevention Systems (IDPS) for IoT.	3
IV	**IoT Security Frameworks and Protocols:** Security Frameworks for IoT: Design principles, architecture of secure IoT systems, NIST-100-2A, IoT-Specific Security Protocols: ZigBee, Bluetooth LE, 6LoWPAN, and their security features, Block-chain for IoT Security: Introduction to Blockchain and its application for secure, decentralized IoT systems, Edge and Fog Computing Security: Security mechanisms in distributed IoT architectures, Threat Modeling and Risk Assessment: Evaluating IoT system vulnerabilities.	3
V	**Real-World IoT Security Case Studies and Applications:** IoT Security in Healthcare: Security and privacy in medical devices, wearable sensors, and health data, IoT Security in Smart Cities: Infrastructure, traffic management, and surveillance systems, Security Challenges in IoT-Enabled Industry 4.0: IoT in manufacturing, robotics, and automation, Designing Secure IoT Solutions: Hands-on project to secure a sample IoT system or application. Case Studies: Real-world security breaches in IoT (e.g., Mirai Botnet, Stuxnet),	3

Text Books	1.	Internet Of Things by Raj Kamal (Author) Publisher-McGraw Hill Education Edition-First Edition, Publication Date-10 March 2017, ISBN-13-978-9352605224
	2.	Security and Privacy in Internet of Things (IoTs): Models, Algorithms, andImplementations by Fei Hu (Author) Publisher-Taylor & Francis Books India Pvt., Edition-1, Publication Date- 29 June 2020, ISBN-13- 978-1032707150
	3.	Privacy and Security in IoT by Harish Chowdhary (Author), Brijesh KumarVerma (Author), Dr. Shaik Mohammad Rafi (Author), Dr. Umesh Sehgal (Author)Publisher-ACADEMIC GURU PUBLISHING HOUSE, Publication Date- 1 January2022, ISBN-13-978-93954689092nd Edition, Pearson, 2004.
E--Books	1.	Security and Privacy in Internet of Things (IoTs) by Fei HU, Publisher -CRC Press Taylor & Francis Group 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742, International Standard Book Number-13: 978-1-4987-2319-0 (eBook - PDF)
	2.	IoT SECURITY GUIDE" By Ministry of Electronics & Information technology Government of India, DSCI, National Center of Excellence, Cyber Security Centre of Excellence Aug-2022
TL Materials	1.	Udemy: Security in IoT (IoT Security) by Parag Achaliya. https://www.udemy.com/course/security-in-iot-
	2.	NPTEL-Internet of Things (IoT)- Prof. Sudip Misra, IIT Kharagpur Duration: 12 weeks https://onlinecourses.nptel.ac.in/noc22_cs96/preview

Department of Computer Science & Engineering (Cyber Security)

Course Title: Network Security										
Semester	VI	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	EVEN	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	MD 4	2	-	-	2	10	15	50		-
Course Code	23BTCYL313									
Teaching Mode	Offline	2 Hrs			Total	75				
Duration of ESE	3 Hrs					75				

Course Objectives	To develop a fundamental understanding of computer and network security proper practices, policies, technologies and standards
	To impart familiarity with the security techniques that provide information and network security
	To evaluate the security of communication systems networks and protocols based on a multitude of security factors
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1 – Describe the fundamental concepts and principles of computer and network security.
	CO2 - Identify and evaluate various network defense mechanisms and security tools.
	CO3 - Implement raw sockets for packet handling and sniffing, and compare key routing algorithms and protocols.
	CO4 - Develop TCP/UDP client–server applications and design iterative, concurrent, and multithreaded server architectures.
	CO5 - Apply symmetric encryption techniques and utilize number theory concepts for pseudorandom generation and stream cipher implementation.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes													
	PO 1	**PO 2**	**PO 3**	**PO 4**	**PO 5**	**PO 6**	**PO 7**	**PO 8**	**PO 9**	**PO 10**	**PO 11**	**PO 12**	**PSO 1**	**PSO 2**
CO1				2									1	
CO2					3									2
CO3				1									2	
CO4					2									3
CO5					3								3	

Course Contents:

Unit	Contents	Hours
I	**Introduction to ISO's OSI Network Architecture:** Internet Model, IP Design and Implementation, Internetworking and routing protocols, Transport layer services and variants, Peer to Peer Networks, Application Layer protocols,	5
II	**Introduction to Network Security and Associated Techniques:** Firewall fundamentals, Firewall features & advanced capabilities,Firewall Design principles, VPNs, Worms, Viruses, Vaccine Programs, Security of Network Layer, Security of Application layer protocols, BSD sockets, Elementary and Advanced system calls.	5
III	**Raw sockets:** Raw Socket Creation, Raw socket output, raw socket input, packet sniffing and routing algorithms: Router IOS- Static and Default Routing-Interior Gateway Routing Protocols: RIP V1&V2, OSPF, EIGRP- Exterior Gateway Routing Protocol: BGP	5
IV	**Introduction to socket programming-** Concurrent Processing in Client-Server, Software-Byte ordering and address conversion functions – Socket Interface - System calls used with sockets - Iterative server and concurrent server- Multi protocol and Multi service server- TCP/UDP Client server programs – Thread Creation and Termination – TCP Echo Server using threads- Remote Procedure Call.	5
V	**Symmetric ciphers:**Classical Encryption Techniques: SubstitutionTechniques, Transposition Techniques, Steganography. Block Ciphers and the Data Encryption Standard, Block Cipher Principles, The Data Encryption Standard. Basic Concepts in Number Theory and Finite Fields: Divisibility and the Division Algorithm, The Euclidean Algorithm. Advanced Encryption Standard, Pseudorandom Number Generation and Stream Ciphers.	5

Text Books	1.	Data Communications and Networking" by Behrouz A. Forouzan
	2.	Cryptography and Network Security: Principles and Practice" by William Stallings
Reference Books	1.	Richards Stevens, Unix network programming, , Vol I & Vol II, 4th edition, Prentice Hall, 2007.
	2.	William Stallings, Cryptography and Network Security, Pearson Education,2007
Online Material	1.	Computer Networking: Principles, Protocols and Practice" by Olivier Bonaventure (Free online resource)

Department of Computer Science & Engineering (Cyber Security)

Course Title: Information Coding Technique										
Semester	VI	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	EVEN	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	VSEC4	1	-	2	2	10	15	-	25	-
Course Code	23BTCYL308/23BTCYP308									
Teaching Mode	Offline				Total	25			25	
Duration of ESE	3 Hr					50				

Course Objectives	**To introduce the fundamental principles of information theory** by explaining the concepts of information, entropy, mutual information, and channel capacity, and to help students understand how information is measured and transmitted efficiently.
	To develop knowledge of coding theory by studying different types of codes, including Huffman codes and convolutional codes, and enabling students to apply these codes through numerical problem-solving
	To provide a strong understanding of cyclic codes by explaining their generation, algebraic structure, and matrix representation, and to train students in solving problems related to cyclic encoding and decoding
	To familiarize students with error detection and correction techniques and enable them to analyze, design, and evaluate basic error control mechanisms through appropriate numerical examples
	To impart knowledge of linear block codes by teaching systematic block code encoding, syndrome computation, and decoding methods, along with developing proficiency in solving related numerical problems.
Course Outcomes	**CO1:** Interpret and apply the fundamental concepts of information theory, including information measure, entropy, mutual information, and channel capacity.
	CO2: Analyze and construct different coding techniques, such as Huffman coding and convolutional coding, and solve numerical problems related to source and channel coding
	CO3: Explain the structure and properties of cyclic codes and perform encoding and decoding using generator polynomials and matrix representations
	CO4: Apply error detection and correction methods to identify, detect, and correct errors in digital communication systems through appropriate numerical techniques
	CO5: Design and evaluate linear block codes using systematic encoding, syndrome decoding, and solve related analytical and numerical problems.

Department of Computer Science & Engineering (Cyber Security)

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1	**3**	**2**	**0**	**1**	**2**	**1**	**0**	**2**	**0**	**1**	**0**	**2**	**3**	**2**	**1**
CO2	**2**	**3**	**2**	**2**	**3**	**1**	**0**	**2**	**0**	**1**	**1**	**2**	**1**	**3**	**1**
CO3	**2**	**2**	**1**	**1**	**2**	**1**	**0**	**1**	**0**	**1**	**0**	**2**	**3**	**2**	**1**
CO4	**3**	**2**	**2**	**2**	**3**	**1**	**0**	**2**	**0**	**1**	**1**	**2**	**2**	**3**	**2**
CO5	**2**	**3**	**2**	**3**	**2**	**1**	**0**	**2**	**1**	**2**	**2**	**3**	**2**	**2**	**3**

Course Contents:

Unit	Contents	Hours
I	**Unit-I:Information Theory** Definition of Information,Measure of Information,Rate of Information,Shannon-Hartley Theorem,Entropy,Relationship between Entropy and Mutual Information.	3
II	**Unit-II:Coding Theory** Classification of Codes,Huffman Coding,Convolutional Coding and Numerical.	3
III	**Unit-III:Cyclic Code** Cyclic Codes Generation,Matrix Description of Cyclic Codes and Numerical.	3
IV	**Unit-IV:Error Detection & Correction Code** Introduction to Error Detection and Error Correction Code and Numerical.	3
V	**Unit-V:Linear Block Codes** Systematic Linear Block Codes encoding,Syndrome decoding and Numerical.	3

Text Books	1.	Thomas M.Cover,Joy A Thomas,Elements of Information Theory,2 nd Edition, Wiley,2015
	2.	Bose,Ranjan.Information theory,Coding and Cryptography,2 nd Edition,Tata McGraw-Hill Education,2008.
	3.	Shu Lin, Daniel J. Costello Jr., *Error Control Coding: Fundamentals and Applications*, 2nd Edition, Pearson, 2004.
E--Books	1.	David J.C. MacKay, Information Theory, Inference, and Learning Algorithms, Cambridge University Press, 2003 (Free Online Edition).
	2.	Raymond W. Yeung, A First Course in Information Theory, Springer, 2002 (Open Access via Chinese University of Hong Kong).
	3.	Rüdiger Urbanke, Tom Richardson, Modern Coding Theory, Cambridge University Press, 2008 (Free Online Draft).
	4.	Igal Sason, Lecture Notes on Information Theory and Coding, Technion – Israel Institute of Technology, 2018 (Free Academic e-Book).
TL Materials	1.	NPTEL, Information Theory and Coding, Video & Web Course, IIT Kharagpur, 2019.
	2.	MIT OpenCourseWare, Information Theory, Lecture Notes & Assignments, Massachusetts Institute of Technology, 2016.
	3.	NPTEL, Digital Communications, Video Lectures & PDFs, IIT Madras, 2018.
	4.	Coursera, Error Control Coding and Information Theory, Online Course Materials, University of Colorado, 2020.

Department of Computer Science & Engineering (Cyber Security)

Practical List

Practical No.	Topic to be covered	COs
1	Implement Coding and Decoding of BCH and RS Codes.	CO1
2	Write a program for determination of various entropies and mutual information of a given channel.Test various types of channel such as CO1 a) Noise free channel b) Error free channel c) Binary Symmetric channel d) Noisy Channel Compare channel capacity of above channels.	CO1
3	Introduction to MATLAB CO2 a) To define and use variables and functions in MATLAB. b) To define and use Vectors and Matrices in MATLAB. c) To study various MATLAB arithmetic operators and mathematical functions. d) To create and use m-files.	CO2
4	Basic plotting of signals CO2 a) To study various MATLAB commands for creating two and three dimensional plots. b) Write a MATLAB program to plot the following continuous time and discrete time signals. i. Step Function ii. Impulse Function iii.Exponential Functions iv. Ramp Function v. Sine Function	CO2
5	Write a MATLAB program to perform amplitude-scaling,time-scaling and time shifting on a given signal.	CO2
6	Write a MATLAB program to obtain linear convolution of the given sequences.	CO2
7	Write a MATLAB program to plot magnitude and phase response of a given system.	CO2
8	Checking linearity/non-linearity of a system using SIMULINK.Build a system that amplifies a sine wave by a factor of two.	CO2
9	Study of Sampling theorem,effect of undersampling.	CO3
10	Sampling of band limited signal:Nyquist theorem.	CO3
11	Sampling of non bandlimited signal: Anti aliasing filter.	CO3
12	Implement a program for generation and evaluation of variable length source coding using Huffman Coding and decoding(C/MATLAB).	CO4
13	Implement coding and decoding of Cyclic codes.	CO4
14	Implement coding and decoding of Convolutional codes.	CO4
15	Implement coding and decoding of Linear block codes.	CO5
16	Write a simulation program to implement source coding and channel coding for transmitting a text file.	CO5
17	Implement a program to study performance of a coded and uncoded communication system (calculate the error probability)	CO5

Course Title: Research Ethics & Technical Writing										
Semester	VI	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	Even	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	RM	-.	-	4 Hrs	2	-	-	-	50	-
Course Code	23BTSHP302CY									

Course Objectives	1. To introduce the basics of scientific communication
	2. To develop skills in scientific writing, ensuring ethical standards
	3. To enable students to identify research problems, formulate objectives and hypotheses
	4. To familiarize students with plagiarism detection tools, ensuring academic integrity and originality in research work.
	5. To provide knowledge on research ethics, intellectual property rights
Course Outcomes	CO1: Explain research fundamentals, hypothesis formulation, and apply appropriate parametric and non-parametric tests.
	CO2: Prepare effective scientific reports and theses using standard structures, tools, and referencing practices.
	CO3: Apply ethical principles and standard norms for writing and publishing research papers in scholarly journals.
	CO4: Identify and formulate research problems and develop structured research proposals with clear objectives and variables.
	CO5: Apply research ethics, IPR concepts, patent drafting and filing procedures, plagiarism control, and responsible publishing practices.

Mapping of Course Outcomes with Program Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes														
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1		3	3	3					3	3					
CO2	3	3	3	3						1					
CO3		3		3						3					
CO4		3	1	3											
CO5				3				3							

Course Contents:

Unit	Contents	Hours
I	**Research Basics:** Meaning and Types. Hypothesis/Assumption: Meaning, Need, Characteristics, Sources, Types (Null & Alternative); and Testing of Hypothesis (Parametric & Non-Parametric Test).	6
II	**Communication Research reports and Thesis writing**: Basics of Communication Skill, Types of Scientific Communication, Introduction: Structure and components of scientific reports, types of report, Thesis writing: different steps and software tools in the design and preparation of thesis, layout, structure and language of typical reports, Illustrations and tables, bibliography, referencing and footnotes.	6
III	**Scientific Writing of Research report:** Ethics of qualitative research and quality of researcher, Research papers: Norms of writing research papers and articles in National and International Journals.	6
IV	**Research Proposal:** Research Proposal: Concept, Need, Importance and Types Research Problem: Meaning, Types, Sources, & Importance; Locating the Research Problem; Criteria for Selecting Research Problem, and Evaluation of Research Problem. Objectives: Concept, Nature and Types. Research variable.	6
V	**Research Ethics, IPR and Publishing:** intellectual property rights and patent law, techniques of writing a Patent, filing procedure, technology transfer, copy right, royalty, trade related aspects of intellectual property rights plagiarism tools: Anti-Plagiarism Software: URKUND …etc., reproducibility and accountability.	6

Text Books	1	Ranjit Kumar, "Research Methodology: A Step by Step Guide for Beginners", SAGE Publications Ltd., 2011.
	2	C.R. Kothari,"Research Methodology: Methods and Trends", New Age International,2004
	3	Gupta S.C, Fundamentals of Statistics, Himalaya Publication House, Bombay Rajaram V. (1996),
E--Books	1	Wayoc C. Booth: The Craft of Research
	2	David Willinson: Research Tools Kits: A Complete Guide to Practitioner Research
Reference Books	1	Wayne Goddard, Stuart Melville, "Research Methodology: An Introduction" JUTA and Company Ltd, 2004.
On line TL Material	1	http:// www.shodhaganga.inflibnet.ac.in
	2	http:// www.inflibnet.ac.in.
	3	http:// www.zotero.org

Sr. No.	Name of Experiments / Mini Projects/ Case Studies
1	Do's and don'ts of user research (CO1)
2	How to write research methodology (CO1)
2	Art of abstract writing (CO2)
3	Writing scientific report (CO2)
4	Accurate referencing (CO2)
5	Oral presentation of research (CO2)
6	Write review paper with proper referencing (CO3)
7	Identifying real life engineering problem (CO4)
8	Preparing proposal of 500 words (CO4)
9	Generating anti-plagiarism report (CO5)
10	Paraphrasing and summarizing to retain originality (CO5).
11	Case study on real world patent dispute (CO5)

Department of Computer Science & Engineering (Cyber Security)

SEMESTER-VII

Course Title: **Applied Cyber Security**										
Semester	VII	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	ODD	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PCC11	3		2	4	10	15	50	25	25
Course Code	23BTCYL401/23BTCYP401									
Teaching Mode	Offline	5			Total	75			50	
Duration of ESE	3 hrs					125				

Course Objectives	This course introduces size and kind of objects.
	1. To understand the basics need of cyber security
	2. To understand the parameters in cyberspace
	3. To understand the security applied at different levels
	4. Understanding computer ethics & security policies Understanding the initiatives taken for cyber security
Course Outcomes	**CO1**: To explain cyberspace & different possible cybercrime.
	CO2: Develop a deeper understanding and familiarity with various types of cyberattacks, cybercrimes, vulnerabilities and remedies thereto
	CO3: To choose the correct browser & applying email security
	CO4: To confirm security while electronic transactions
	CO5: To understand & apply for security policies & explore more initiatives

Department of Computer Science & Engineering (Cyber Security)

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes													
	PO1	PO2	PO3	PO4	PO5	PO6	PO 7	PO 8	PO9	PO10	PO11	PO 12	PS O 1	PS O 2
CO1	-	3	-	-	-	-	-	-	-	-	-	-	3	-
CO2	-	3	2	-	-	-	-	-	--	-	-	-	2	-
CO3	-	1	3	-	-	-	-	-	-	-	-	-	-	3
CO4	-	1	3	-	-	-	-	-	--	-	-	-	-	-
CO5	-	1	3	-	-	3	-	-	-	-	-	-	--	3

Course Contents:

Unit	Contents	Hours
I	**Introduction to Cyber security** Defining Cyberspace and Overview of Computer and Web-technology, Architecture of cyberspace, Concept of cyber security scope of cybersecurity, Cybersecurity Goals Regulation of cyberspace, Issues and challenges of cyber security, Cybersecurity Tools, Internet Security Concepts HTTPS and secure websites, Introduction to Ethical Hacking Difference between Red Team (attackers) and Blue Team (defenders)	8
II	**Cybercrime** Cybercrimes targeting Computer systems and Mobiles- data diddling attacks, spyware, logic bombs, DoS, DDoS, APTs, virus, Trojans, ransomware, data breach., Online scams and frauds- email scams, Phishing, Vishing, Smishing, Online job fraud, Online sextortion, Debit/ credit card fraud, Online payment fraud, Cyberbullying, website defacement, Cyber- squatting, Pharming, Crypto jacking, Darknet- illegal trades, Social Media Scams & Frauds- impersonation, identity theft, job scams, misinformation, fake newscyber crime against persons - cyber grooming, cyber stalking., Social Engineering attacks,Monitoring log analysis, threat Intelligent Case studies	8
III	**Cyber Laws** Cyberc rime and legal landscape around the world, IT Act, 2000 and its amendments. Limitations of IT Act, 2000. Cybercrime and punishments, Cyber Laws and Legal and ethical aspects related to new technologies- AI/ML, IoT, Blockchain, Darknet and Social media, Cyber Laws of other countries, Data protection, Data privacy and data security, Data protection principles, Big data security issues and challenges, Data protection regulations of other countries- General Data Protection Regulations(GDPR),2016 Personal Information Protection and Electronic Documents Act (PIPEDA)., Social media- data privacy and security issues, Case Studies.	8 8

IV	**Cyber Security Industry Standards** Threat Handler, Role of threat handler , Tools Used by threat handlers, ISO 27701 std Relationship between ISO 27001, ISO 27002, and ISO 27701, Purpose of PIMS, NISP Purpose and importance of NISP, Components of NISP, Zero Trust Architecture(ZTA) Frameworks & Standards Zero Trust vs. Traditional Security ,Zero Trust Components, Resilience, Difference Between Security and Resilience, Key Aspects of Cybersecurity Resilience Case study on GDPR compliance using ISO 27701	
V	**Cyber security Management Compliance and Governance** Cyber security Plan- cyber security policy, cyber crises management plan., Business continuity, Risk assessment, Types of security controls and their goals, Cyber security audit and compliance, National cyber security policy and strategy**.** PCI-DSS History and purpose, PCI-DSS Compliance Process Case Studies	8

Text Books	1.	"Introduction to Cyber Security: Fundamentals" Ugo Ekpo (MBCS CITP), Independently published (October 12, 2018)
E-Books	1.	Cybersecurity: The Beginner's Guide A Comprehensive Guide to Getting Started in Cybersecurity, Erdal Ozkaya
Reference Books	1.	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd.
	2.	Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform.
	3.	Information Warfare and Security by Dorothy F. Denning, Addison Wesley.

Department of Computer Science & Engineering (Cyber Security)

Practical list (Course Code 23BTCYP401)

1	To collect publicly available information about a target using OSINT **(**Open Source Intelligence.) tools.
2	To collect intelligence about a target using open-source tools like Maltego, Shodan, the Harvester.
3	To demonstrate how phishing emails trick users and collect credentials.
4	To detect suspicious activities by analyzing logs.
5	To configure and test firewall rules for blocking unauthorized access.
6	To capture and analyze network packets for suspicious behavior.
7	To configure automated backups and restore data after a failure.
8	To test recovery procedures during system or network outage.
9	To simulate a ransomware attack and restore systems without paying ransom.
10	To create dashboards and alerts for threat monitoring.

Course Title: Advanced Information Security										
Semester	7th	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	Odd	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PCC12	3	-	-	3	10	15	50	-	-
Course Code	23BTCYL403									
Teaching Mode	Offline	3			Total	75				
Duration of ESE	3 Hr					75				

Course Objectives	Understand advanced cyber-attack methodologies
	Gain proficiency in network security mechanisms
	Acquire strong foundational and practical knowledge of modern cryptographic techniques
	Explore and apply artificial intelligence and machine learning techniques
Course Outcomes	CO1: Explain advanced cyber-attack strategies
	CO2: Analyze network traffic and detect intrusions using IDS/IPS, deep packet inspection,
	CO3: Apply modern cryptographic algorithms and security protocols
	CO4: Evaluate security risks in cloud and virtualized infrastructures and implement security mechanisms
	CO5: Develop and implement AI/ML-based security solutions for threat detection

Department of Computer Science & Engineering (Cyber Security)

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1	**3**	**2**	**0**	**1**	**2**	**1**	**0**	**2**	**0**	**1**	**0**	**2**	**3**	**2**	**1**
CO2	**2**	**3**	**2**	**2**	**3**	**1**	**0**	**2**	**0**	**1**	**1**	**2**	**1**	**3**	**1**
CO3	**2**	**2**	**1**	**1**	**2**	**1**	**0**	**1**	**0**	**1**	**0**	**2**	**3**	**2**	**1**
CO4	**3**	**2**	**2**	**2**	**3**	**1**	**0**	**2**	**0**	**1**	**1**	**2**	**2**	**3**	**2**
CO5	**2**	**3**	**2**	**3**	**2**	**1**	**0**	**2**	**1**	**2**	**2**	**3**	**2**	**2**	**3**

Course Contents:

Unit	Contents	Hours
I	**Advanced Threats & Attack Techniques** – -Advanced Persistent Threats (APT): Understanding long-term cyber infiltration strategies. - Fileless Malware Attacks: How malware operates without traditional files. - Ransomware & Rootkits: How attackers encrypt data and maintain hidden access. - Zero-Day Exploits: Identifying and defending against unknown vulnerabilities. *Case Study:* Advanced Persistent Threat (APT) – "Operation Aurora"	7
II	**Network Security & Intrusion Detection** – -Intrusion Detection Systems (IDS) & Intrusion Prevention Systems (IPS). - Deep Packet Inspection & Traffic Analysis. - Securing Wireless Networks & Preventing Man-in-the-Middle Attacks. - Configuring Firewalls (FortiGate, Cisco, pfSense). *Case Study*: Traffic Analysis of a DDoS Attack Using Wireshark	8
III	**Cryptography & Secure Communication** – -Advanced Encryption Techniques: AES, RSA, ECC. - Digital Signatures & Hashing: SHA-256, MD5. - Secure Email & Messaging Protocols: PGP, S/MIME. - Blockchain Security & Zero-Knowledge Proofs. *Case Study:* Securing Sensitive User Data using AES-256 Encryption	7
IV	**Cloud & Virtualization Security** - Understanding Cloud Service Models (IaaS, PaaS, SaaS). - Cloud Security Threats & Risk Management. - Zero Trust Architecture & Identity Access Management (IAM). - Securing Virtual Machines (VMs) & Containers (Docker, Kubernetes). - Hands-On: Setting up multi-factor authentication in cloud environments, implementing security policies in AWS/Azure.	7
V	**AI & Machine Learning in Cyber Security** – -AI-Driven Threat Detection & Response. - Machine Learning Algorithms for Cybersecurity.	8

	- Deep Learning for Anomaly Detection. - Defending Against AI-Powered Cyber Attacks. - Hands-On: Using Python for building basic threat detection models, implementing AI-based security monitoring	

Book	Author(s)	Edition & Year	Publisher	ISBN / Notes
Cryptography & Network Security: Principles & Practice	William Stallings	8th Edition (2023) (Pearson Education)	Pearson Education	ISBN: 9789357059718 (Pearson Education)
Applied Cryptography: Protocols, Algorithms and Source Code in C	Bruce Schneier	2nd Edition, 2015 (Google Books)	John Wiley & Sons	ISBN: 9781119096726 (Google Books)
Security Engineering: A Guide to Building Dependable Distributed Systems	Ross J. Anderson	3rd Edition, 2020 (VitalSource)	John Wiley & Sons	ISBN-13: 9781119642787 (VitalSource)
Cyber Security Foundations: Fundamentals, Technology and Society	Keith Martin, Konstantinos Mersinas, Guido Schmitz & Jassim Happa	Kogan Page, 1st Edition (2025). ISBN: 9781398614727.		
Principles of Information Security	Michael E. Whitman & Herbert J. Mattord	Course Technology (widely used textbook).		

Department of Computer Science & Engineering (Cyber Security)

Course Title: Web Technology										
Semester	VII	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	ODD	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PCC13	2	-	2	4	10	15	50	25	25
Course Code	23BTCYL404 / 23BTCYP404									
Teaching Mode	Offline	4 Hrs			Total	75			50	
Duration of ESE	3 Hrs					125				

Course Objectives	Students will able to understand and illustrate HTML.	
	Students will be able to understand about XML, Dynamic HTML Properties.	
	Student will able to understand basic of Java Scrip	
	Student will able to design website.	
Course Outcomes	Up on successful completion of this course, student will be able to:	
	CO1	Understand basic principles of dynamic interactive web sites.
	CO2	Apply the different tags of HTML, CSS, and XHTML.
	CO3	Analyze various scripting languages to create interactive components in web pages.
	CO4	Design and implement dynamic websites with good aesthetic sense
	CO5	Understanding Semantic Web and Applying Web Analytics over Semantic Web.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1		**1**		**3**				**2**		**2**		**3**	**3**	
CO2			**2**	**1**	**3**							**3**		**2**
CO3		**1**		**2**	**3**							**3**	**1**	
CO4		**3**									**1**	**2**		
CO5				**1**	**3**							**2**		

Course Contents:

Unit	Contents	Hours
I	**Internet and World Wide Web** - Overview, Web System Architecture, Web Clients and Web Servers, Application Servers. Hypertext Transfer Protocol - primitives, methods, content transport, HTTP1.1 and HTTP2, HTTPS, SSL. Introduction to HTML: HTML Common tags- List, Tables, images, forms, Frames; Cascading, Style sheets. Client side programming with XHTML, HTML5, CSS3.	6
II	**Dynamic HTML:** Introduction, Object Referencing, Dynamic Styles, Dynamic Positioning, Using the frames Collection, navigator Object, Summary of the DHTML Object Model, Event Model. XML: Introduction to XML, Defining XML tags, their attributes and values, Document type definition, XML Schemas, Document Object model, XHTML, XPath and XSLT	7
III	**JavaScript: Functions**- Introduction, Data types, Variables, Expressions and Operators. JavaScript Statements, loops, arrays, strings, function, JavaScript Global Functions, Recursion, javaScript arrays, JavaScript objects. Event driven programming with JavaScript, Client-side validation; Server side programming, Sessions and Session Tracking techniques, **API Call and API endpoints, Rest API.**	6
IV	**PHP :** Starting to script on server side, Arrays, function and forms, advance PHP Databases : Basic command with PHP examples, Connection to server, creating database, selecting a database, listing database, listing table names creating a table, inserting data, altering tables, queries, deleting database, deleting data and tables, PHP myadmin and database bugs.	7
V	**Service Oriented Architecture** – SOAP. Web 2.0 technologies, Introduction to semantic web. Capturing Information from semantic web pages; Data analytics over semantic and linked Web. Internet/Web of Things, Applications and Research Trends.	7

Text Books	1	Web Developer's Reference Guide. By: Joshua Johanan, Talha Khan, Ricardo Zea
	2	Bai and Ekedhi, The Web Warrior Guide to Web Programming, 3rd Edition, Thomson, 2008.
E-Books	1	https://www.wileyindia.com/web-technologies-html-javascript-php-java-jsp-asp-net-xml-and-ajax-black-book.html
	2	https://www.pdfdrive.com/web-developers-reference-guide-e158159681.html
Reference Books	1	Deitel, Deitel and Nieto, Internet and Worldwide Web - How to Program, 5th Edition, PHI, 2011.
	2	G. Antoniou, P. Groth, F. Harmelen and R. Hoekstra, “A Semantic Web Primer” Prentice Hall India
On line TL Material	1	W3 School web Development: https://www.w3schools.com/whatis/whatis_icons.asp
	2	https://www.geektonight.com/web-technologies-notes-pdf/

Department of Computer Science & Engineering (Cyber Security)

List of Experiment

Sr.No.	Experiment List	Mapping With CO
1	Introduction to HTML, Skelton of HTML, Project Folder Structure, HTML File Extension, Editor Installation Developing First HTML Page	CO1
2	Introduction to Tags, Elements & Attributes, HTML Tags, Presentational Tags, Headings, Paragraph, List, Image, Anchor	CO1
3	Implementation Tables, Scope of CSS and Implementation, Understand the HTML Coding Standard	CO2
4	Implementation of DIV tag and its usage, CSS properties, Box Model	CO2
5	Implementation of Java Script and Jquery	CO3
6	Introduction to PHP, Client Server Architecture, Client side and Server side Script, Syntax of PHP, Variable Declaration, Result & Errors in PHP	CO4
7	Implementation of String, Constants, Operators and Conditional Statements with Following 3 Programing Execution 1. Write a php code to check number is even or odd 2. Write a php code to check is eligible to vote or not 3. Write a php code to check given number is positive negative or zero	CO4
8	Implementation of looping statement, Array, Sorting Function Using Array, with following 3 programs in Looping and Array 1. Write a php code to generate Armstrong Number 2. Write a php code to generate Prime Number 3. Write a php code to generate bubble sort.	CO4
9	Implementation of connection to PHP and MySql, DB Connection String, retrieval of Database table on the HTML Page.	CO4
10	CRUD operation in PHP and MySQL, Develop and web application using crud operation	CO5
11	Open Ended Mini Project	CO1, CO2, CO3, CO4, CO5

Course Title: **Computer Vision**										
Semester	VII	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	ODD	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PE-IV-1	4		--	4	10	15	50	--	--
Course Code	23BTCYL408									
Teaching Mode	Offline	4			Total	75			--	
Duration of ESE	3 hrs					75				

Course Objectives	To build a strong foundation in computer vision concepts and image formation.
	To understand classical and modern image processing techniques.
	To apply computer vision in cybersecurity domains such as surveillance, biometrics, and anomaly detection.
Course Outcomes	**CO1:** Explain fundamental concepts of computer vision and image formation.
	CO2: Apply image processing techniques for enhancement and filtering.
	CO3: Extract and analyze features using classical and modern methods.
	CO4: Implement motion analysis and tracking algorithms.
	CO5: Design solutions for real-world problems using deep learning-based vision models.

Mapping of Course Outcomes with Program Outcomes

Course Outcomes	Program Outcomes and Program Specific Outcomes											
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**
CO1	0	0	2	0	0	2	0	0	0	0	0	0
CO2	2	0	2	0	2	1	2	0	2	0	0	0
CO3	1	0	1	2	0	1	0	3	0	0	2	0
CO4	2	0	1	2	2	1	1	0	0	0	2	0
CO5	0	3	0	1	0	2	0	0	0	0	0	3

Course Contents:

Unit	Content	Hours
I	**Fundamentals of Computer Vision** Introduction to Computer Vision & Applications, Image Formation & Representation, Camera Models & Geometry, Radiometry & Image Digitization, Transformations: Rigid, Affine & Perspective, Introduction to OpenCV.,Image formation pipeline algorithm, Camera projection (Pinhole model) **Lab Assignment:** • Implement Histogram Equalization using Python/OpenCV	7
II	**Image Processing Techniques** Pixel & Intensity Transformations, Color Models (RGB, HSV, YCbCr) , Histogram Processing & Equalization, Spatial Filtering & Convolution , Frequency Domain (Fourier Transform), Noise Removal & Image Enhancement,Histogram Equalization algorithm, K-Means Clustering for segmentation **Lab Assignment:** • Feature matching using ORB/SIFT	7
III	**Feature Detection & Image Segmentation** Edge Detection (Sobel, Canny), Corner Detection (Harris, FAST), Feature Descriptors: SIFT, SURF, HOG, Shape Representation Techniques,**FAST Algorithm Segmentation Techniques:** Thresholding & Region-based methods**,** Watershed Algorithm, Graph-based Segmentation, Mean Shift & Normalized Cuts, K-Means Clustering for segmentation, Mean Shift algorithm **Lab Assignment:** • Motion detection in video streams	8
IV	**Motion Analysis, Camera Calibration & Deep Learning** Camera Calibration (Intrinsic & Extrinsic Parameters), Lens Distortion Correction, Motion Representation & Optical Flow, Motion Estimation Techniques, Feature-based Tracking. **Deep Learning for Computer Vision:** Introduction to Neural Networks, Convolutional Neural Networks (CNN), Transfer Learning **Algorithms: CNN** Architecture (LeNet, AlexNet), Transfer Learning (ResNet, VGG), Image Classification Models.	7
V	**Advanced AI Applications in Security (IAM & VM Focus)** AI in Identity & Access Management (IAM), Vision Models (VM) in Security Systems, Ethical Issues in AI Security **Advanced Algorithms Added Deepfake Detection:** CNN-based Deepfake Detection, XceptionNet for fake video detection, **Biometric Anti-Spoofing:**Face liveness detection, CNN-based fingerprint/face spoof detection, **Adversarial AI Attacks:** FGSM (Fast Gradient Sign Method), PGD (Projected Gradient Descent)	8

Text Books	1	Szeliski, R. – *Computer Vision: Algorithms and Applications*
	2	Goodfellow et al. – *Deep Learning* (Selected chapters)
	3	Richard Szeliski (Latest Online Edition recommended)
Reference Books	1	Trucco & Verri – *Introductory Techniques for 3D Computer Vision*
	2	Forsyth & Ponce – *Computer Vision: A Modern Approach*
	3	Ian Goodfellow – *Deep Learning*
Online TL Material	1	NPTEL: Computer Vision Courses
	2	Coursera: Deep Learning Specialization

Department of Computer Science & Engineering (Cyber Security)

Course Title: Evidence Acquisition and Recovery (E-IV)										
Semester	VII	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term		Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PE- IV	4	-	-	4	10	15	50	NA	NA
Course Code	23BTCYL405									
Teaching Mode	Offline	4Hrs			Total	75			–	
Duration of ESE	3 Hrs					75				

Course Objectives	To understand digital data and evidence acquisition techniques.
	To analyze digital evidence through identification, acquisition, and preservation methods.
	To learn digital forensic investigation and data recovery techniques.
Course Outcomes	Upon successful completion of this course, student will be able to:
	CO1: Understand the fundamental concepts and components of digital data
	CO2: Design the principles of digital evidence and the role of digital forensics in investigations.
	CO4: Analyze digital evidence using forensic tools.
	CO5: Implement data recovery and evidence preservation techniques.

Mapping of Course Outcomes with Program Outcomes:

Course Outcomes	Program Outcomes												PSO		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	2	1			3								3	3	2
CO2	3	2		2									3	3	3
CO3	3		2		3								3	3	3
CO4	2	3	3		2								3	3	3
CO5	2		2		3			1					3	3	3

Course Contents:

Unit	Contents	Hours
I	**Introduction to Digital Data Systems** Introduction to Digital Data Systems , Introduction to Digital Forensics and Digital Evidence , Importance and Types of Digital Evidence ,Digital Forensic Investigation Frameworks and NIST Model , Identification, Collection, Securing and Seizing of Digital Evidence , Evidence Preservation and Chain of Custody Basics , Storage Formats for Digital Evidence – Raw Format and Advanced Forensic Format (AFF) , Data Acquisition Methods and Tools ,Validation of Data Acquisition using Hashing Techniques ,Volatile and Non-Volatile Memory Concepts , Introduction to Memory Forensics ,Introduction to Cloud Forensics , Introduction to Forensic Tools – Autopsy and Other Open-Source Tools	8
II	**Digital Evidence** Digital Evidence and Types of Digital Evidence, Challenges in Acquiring Digital Evidence, Admissibility of Evidence, Chain of Custody, Digital Forensics Examination Process – Seizure, Acquisition, Analysis and Reporting, Forensic Image Formats, Live and Static Acquisition Techniques.	8
III	**Data Acquisition and Evidence Gathering** Data Acquisition from Live, Shutdown and Remote Systems, E-mail Investigation Basics, Password Cracking Concepts, Mobile Device Seizure and Preservation, Data Acquisition from Mobile Devices and Social Media, Acquisition of Encrypted Systems, Challenges in Cybercrime Investigation.	8

IV	**Analysis of Digital Evidences** Search and Seizure of Digital Evidence, Imaging and Hashing Techniques, Deleted File Recovery Basics, Introduction to Steganography and Steganalysis, Open Source and Proprietary Forensic Tools, Importance of Log Analysis in Forensic Investigation.	7
V	**Data Recovery** Duplication and Preservation of Digital Evidence, Data Recovery Tools and Procedures Recovery of Deleted Files and Formatted Partitions, Recovery of Internet Usage Data and Temporary Files, Data Backup and Recovery Techniques , Ethics and Legal Considerations in Data Recovery, Introduction to Mobile Data Recovery Techniques, Case Studies on Digital Evidence Acquisition and Recovery.	7

Text Books	1.	ADVANCED DIGITAL FORENSICS: Techniques and Technologies for 2024 Covers modern digital forensic techniques, evidence acquisition, malware analysis, cloud and mobile forensics. Suitable for updated cyber security curriculum.
	2.	Digital Forensics and Incident Response Focuses on incident response, forensic investigation procedures, evidence analysis, and cyber threat response.
	3.	Digital Forensics and Incident Response: A practical guide to using Kali Linux for cyber investigations Includes practical forensic investigation using Kali Linux, FTK Imager, Volatility, and Autopsy tools.
	4.	Digital Forensics with Kali Linux Useful for evidence acquisition, hashing, data recovery, and network forensics using open-source forensic tools.
	5.	Laws of Electronic Evidence and Digital Forensics Covers legal aspects, admissibility of evidence, chain of custody, and ethical considerations in digital forensics.
Reference Book	1.	Practical Digital Forensics: A Guide for Windows and Linux Users Practical guide covering live acquisition, file system forensics, browser forensics, and forensic reporting.
	2.	Advances in Digital Forensics XX Advanced reference book discussing recent research trends in mobile, malware, and IoT forensics.
	3.	Digital Forensics, Investigation, and Response Good reference for investigation procedures, evidence handling, and forensic methodologies.
	4.	Learn Computer Forensics Beginner-friendly reference book for understanding forensic investigation concepts and tools.
	5.	The Art of Memory Forensics Standard reference for memory forensics and malware investigation techniquesLNJN National Institute of Criminology and Forensic Science, “A Forensic Guide for Crime Investigators – Standard Operating Procedures”.

Course Title: Cyber Threat Investigation & Forensics										
Semester	VII	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	ODD	Th	Tu	Pr	Credits	AE	AE	SE	INT	EXT
Course Category	MD5	4	-	-	4	10	15	50	-	-
Course Code:	23BTCYL424									
Teaching Mode	Offline	4 Hrs			Total	75			-	
Duration of ESE	3 Hrs					75				

Course Objectives	To correctly define and cite appropriate instances for the application of computer forensics Correctly collect and analyze computer forensic evidence.
	Identify the essential and up-to-date concepts, algorithms, protocols, tools, and methodology of Computer Forensics.
	To investigate attacks, IDS. Technical exploits and router attacks and “Trap and Trace” computer networks.
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1: Demonstrate the principles of Network & Cyber Forensics and how resultant evidence can be applied within legal cases.
	CO2: Illustrate their competence in recovering files, network forensics, traffic analysis
	CO3: Evaluate the effectiveness of available network & cyber forensics tools and use them in a way that optimizes the efficiency and quality of network & cyber forensics investigations.
	CO4: Apply a solid foundational grounding in computer networks, operating systems, file systems, hardware, and mobile devices to digital investigations and to the protection of computer network resources from unauthorized activity
	CO5: Access and critically evaluate relevant technical and legal information of email and emerging industry trends

Department of Computer Science & Engineering (Cyber Security)

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO9	PO10	PO11	PO12	PSO 1	PSO 2
CO1		**1**		**3**				**2**		**2**		**3**	**3**	
CO2			**2**	**1**	**3**							**3**		**2**
CO3		**1**		**2**	**3**							**3**	**1**	
CO4		**3**									**1**	**2**		
CO5				**1**	**3**							**2**		

Course Content:

Unit	Contents	Hours
I	Introduction to Cyber Forensics, Use of Computer Forensics in Law Enforcement, Computer Forensics Assistance to Human Resources/Employment Proceedings, Computer Forensics Services, Benefits of professional Forensics Methodology, Steps taken by Computer Forensics Specialists, Introduction to IDS and IPS, Network forensic overview, TCP/IP fundamentals.	5
II	An Overview Of Network Forensics Investigation, privacy, security and legal issues on computer networks and the internet, Procedures for network forensics, Understanding Traffic Analysis Scanning –Port Scanning, Network Scanning, Vulnerability Scanning	5
III	TCP vs UDP, application protocols, the OSI model, IP addressing, NAT Network Intrusions And Cyber Crime, Investigating Network Intrusions and Cyber Crime, Network Forensics and Investigating logs, network packet capture tools – Wireshark, Checking of Live system using IP Scanner and Ping Sweep.	5
IV	Cyber Forensics, Standards, Guidelines and Best Practices- Handling the Digital Crime Scene, Digital Evidence Examination Guidelines –ACPO, Daubert guidelines, Cyber forensics tools. MITRE ATT&CK, SIEM-based investigation and case studies	5
V	E-mail Forensics, Exploring the role of email investigation, Exploring the role of client and server in email, Investigating E-mail crimes and violations, Examining E-mail Messages, Viewing E-mail headers, Examining Email headers, Examining additional E-mail files, Tracing an e-mail message, using network E-mail logs, Understanding E-mail servers, case studies	5

Text Books	1. C. Altheide& H. Carvey Digital Forensics with Open Source Tools, Syngress, 2011. ISBN: 9781597495868.
Online learning Material	Online Course management System: https://esu.desire2learn.com/

Department of Computer Science & Engineering (Cyber Security)

Course Code	Name of Course	Course Category	Teaching Scheme				Credits	Evaluation Scheme					
								Theory			Practical		Total Marks
			L	T	P	Total Hours		TAE	CAE	ESE	INT	EXT	
SEMESTER-VIII													
23BTCYL4XX	PE-V (MOOCs based)	PEC5	4			4	4	10	15	50			75
23BTCYP418	Internship	I			24	24	12				200	100	300
TOTAL			**4**		**24**	**28**	**16**	**10**	**15**	**50**	**200**	**100**	**375**