SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

Department of Computer Science and Engineering (Cyber Security)

SCHEME FOR BACHELOR OF TECHNOLOGY (B. Tech)

COMPUTER SCIENCE & ENGINEERING

(Cyber Security)

Batch 2025-2029

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

SCHEME - B. TECH – III SEM

SL	COURSE CODE	COURSE TITLE	SCHEME OF TEACHING					Examination (Maximum Marks)		
			L	T	P	J	C	CIE	SEE	TM
1		Applied Statistics & Stochastic Processes	3	0	0	0	3	60	40	100
2		Data Structures and Algorithms	3	0	2	0	4	60	40	100
3		Digital Logic and Computer Organization	3	0	2	0	4	60	40	100
4		Computer Networks	3	0	2	0	4	60	40	100
5		Cyber Security Essentials *	3	0	0	0	3	60	40	100
6		Sustainability Engineering & Environmental Social and Governance	2	0	0	0	2	60	40	100
7		Skill Enhancement Course-I (Choice of Courses)	1	0	2	0	2	100	--	100
8		Cognitive and Technical Skills-III		-	-	-	P/F	-	-	--
			18	0	8	0	22	460	240	700

L – Lecture, T – Tutorial, P – Practical, J – Project, C – No. of Credits, CIE – Continuous Internal Evaluation,

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

SEE- Semester End Examinations, TM – Total Marks.

* The syllabus shall be furnished by Cyberbit

** The syllabus shall be furnished by NVIDIA

Skill Enhancement Course-I	
COURSE CODE	**COURSE NAME**
	Discrete Mathematics
	Linux Programming

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

SCHEME - B. TECH –IV SEM

SL	COURSE CODE	COURSE TITLE	SCHEME OF TEACHING					Examination (Maximum Marks)		
			L	T	P	J	C	CIE	SEE	TM
1		Differential Equations & Optimization	3	0	0	0	3	60	40	100
2		Cloud Security*	3	0	0	0	3	60	40	100
3		Embedded System Design	3	0	2	0	4	60	40	100
4		Design Studio II: Open Source Tools in Cyber Security	1	0	0	2	2	60	40	100
5		Introduction to Data Science	2	0	0	0	2	60	40	100
6		AI Essentials for Cyber Security*	3	0	2	0	4	60	40	100
7		Liberal Studies (Humanities / Social Science)	2	0	0	0	2	100	-	100
8		Skill Enhancement Course II	1	0	2	0	2	100	-	100
9		Cognitive and Technical Skills-IV		-	-	-	P/F	-	-	--
			19	0	4	2	22	560	240	800

L – Lecture, T – Tutorial, P – Practical, J – Project, C – No. of Credits, CIE – Continuous Internal Evaluation,

SEE- Semester End Examinations, TM – Total Marks.

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

Skill Enhancement Course II	
COURSE CODE	**COURSE NAME**
	Web Technologies
	DevOps

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

SCHEME - B. TECH –V SEM

SL	COURSE CODE	COURSE TITLE	SCHEME OF TEACHING					Examination (Maximum Marks)		
			L	T	P	J	C	CIE	SEE	TM
1		Responsible AI, Ethics & Policy	2	0	0	0	2	60	40	100
2		Deep Learning	3	0	2	0	4	60	40	100
3		Forensics Fundamentals *	3	0	0	0	3	60	40	100
4		Database Management Systems	3	0	2	0	4	60	40	100
5		Sustainability for Cyber Physical Systems /MOOC/NPTEL	2	0	0	0	2	60	40	100
6		Design Studio III: Innovation, Design Thinking & IP	1	0	0	2	2	100	-	100
7		Professional Elective-I / MOOC	3	0	0	0	3	60	40	100
8		Cognitive and Technical Skills-V		-	-	-	P/F	-	-	--
			17	0	4	2	20	460	240	700

L – Lecture, T – Tutorial, P – Practical, J – Project, C – No. of Credits, CIE – Continuous Internal Evaluation,

SEE- Semester End Examinations, TM – Total Marks.

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

Professional Elective Course- I	
COURSE CODE	**COURSE NAME**
	AI-Driven Hardware Security
	Criminal Psychology and Behavior Intelligence
	Application Security
	Cyber Law, Ethics & Governance
	Basic Windows / Linux/ MAC Security*
	Computer Vision Fundamentals **

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

SCHEME - B. TECH –VI SEM

SL	COURSE CODE	COURSE TITLE	SCHEME OF TEACHING					Examination (Maximum Marks)		
			L	T	P	J	C	CIE	SEE	TM
1		Adversarial Machine Learning	3	0	2	0	4	60	40	100
2		Operating Systems	3	0	0	0	3	60	40	100
3		Vulnerability Analysis and Penetration Testing*	3	0	2	0	4	60	40	100
4		Cyber Risk Management	2	0	0	0	2	60	40	100
5		Professional Elective II / MOOC	3	0	0	0	3	60	40	100
6		Mini Project (CoE-based / Startup / Research Track)	0	0	0	4	2	100	-	100
7		Open Elective -I	3	0	0	0	3	60	40	100
8		Cognitive and Technical Skills-VI		-	-	-	P/F	-	-	--
			17	0	4	4	21	460	240	700

L – Lecture, T – Tutorial, P – Practical, J – Project, C – No. of Credits, CIE – Continuous Internal Evaluation,

SEE- Semester End Examinations, TM – Total Marks

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

Professional Elective II	
COURSE CODE	**COURSE NAME**
	AI for IoT & IIoT Security
	Disk & Memory Forensics
	Secure Coding
	Ethical Hacking
	Security Analyst Tier-1*
	Advanced Data Science**

Open Elective I	
COURSE CODE	**COURSE NAME**
	Networks Security Essentials
	Cyber Security Essentials

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

SCHEME - B. TECH – VII SEM

SL	COURSE CODE	COURSE TITLE	SCHEME OF TEACHING					Duration in Hrs Exam	Examination (Maximum Marks)		
			L	T	P	J	C		CIE	SEE	TM
1		Entrepreneurial Finance and Deep tech Startups	2	0	0	0	2	3	100	--	100
2		Cryptography and Network Security*	3	0	0	0	3	3	60	40	100
3		Professional Elective III	3	0	0	0	3	3	60	40	100
4		Professional Elective IV	3	0	0	0	3	3	60	40	100
5		Open Elective II	3	0	0	0	3	3	60	40	100
6		Capstone Project I (Problem Definition & Design)	0	0	0	8	4	1	60	40	100
			14	0	0	8	18	16	400	200	600

L – Lecture, T – Tutorial, P – Practical, J – Project, C – No. of Credits, CIE – Continuous Internal Evaluation,

SEE- Semester End Examinations, TM – Total Marks

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

Professional Elective Course - III	
COURSE CODE	**COURSE NAME**
	AI in Quantum Cryptography
	Network Forensics
	Big Data Security
	Security Engineering and Cyber Defense
	Security Analyst Tier-2*
	Generative AI Application & LLM**

Professional Elective Course - IV	
COURSE CODE	**COURSE NAME**
	AI-Powered Data Center Security
	Mobile & IoT Forensics
	Operating Systems Security
	Cyber Risk Analytics & Management
	Security Auditing & Compliance *
	Agentic AI Security **

Open Elective Course- II	
COURSE CODE	**COURSE NAME**
	Cryptography
	Digital Forensics

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

SCHEME - B. TECH – VIII SEM

SL	COURSE CODE	COURSE TITLE	SCHEME OF TEACHING					Exam Examination (Maximum Marks)		
			L	T	P	J	C	CIE	SEE	TM
1		Professional Elective V / MOOC	3	0	0	0	3	60	40	100
2		Leadership, Policy & Authentic Intelligence, Societal Impact Engineering **(**CSE)	2	0	0	0	2	100	--	100
3		Internship (Industry / Research / CoE based)	0	0	4	0	2	100	-	100
4		Capstone Project II (Build, Deploy & Impact)	0	0	0	20	10	60	40	100
			5	0	4	20	17	320	80	400

L – Lecture, T – Tutorial, P – Practical, J – Project, C – No. of Credits, CIE – Continuous Internal Evaluation,

SEE- Semester End Examinations, TM – Total Marks

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

Professional Elective Course- V	
COURSE CODE	**COURSE NAME**
	AI in Automotive Security
	Advanced Forensics & Legal Expertise
	Blockchain Technology
	Endpoint Security
	Security Analyst Tier-3 *
	Industrial Digital Twins**

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

Minor Degree in Information Security

SCHEME - B. TECH – 2026-27

SL	COURSE CODE	COURSE TITLE	SCHEME OF TEACHING					Exam Examination (Maximum Marks)		
			L	T	P	J	C	CIE	SEE	TM
1		Ethical Hacking (Sem- IV)	3	0	0	0	3	60	40	100
2		Cloud Security (Sem- V)	3	0	0	0	3	60	40	100
3		Blockchain Technology (Sem- VI)	3	0	0	0	3	60	40	100
4		Cryptography and Network Security (Sem- VI)	3	0	0	0	3	60	40	100
5		Cybersecurity Governance, Risk and Compliance (Sem- VII)	3	0	0	0	3	60	40	100
6		Hardware Security (Sem- VII)	3	0	0	0	3	60	40	100

L – Lecture, T – Tutorial, P – Practical, J – Project, C – No. of Credits, CIE – Continuous Internal Evaluation, SEE- Semester End Examinations, TM – Total Marks

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

Honours Degree

SCHEME - B. TECH – 2026-27

SL	COURSE CODE	COURSE TITLE	SCHEME OF TEACHING					Exam Examination (Maximum Marks)		
			L	T	P	J	C	CIE	SEE	TM
1		Zero Trust Security Architecture (Sem V)	3	0	0	0	3	60	40	100
2		Digital Identity & Privacy Engineering (Sem V)	3	0	0	0	3	60	40	100
3		Smart Grid & Critical Infrastructure Security (Sem VI)	3	0	0	0	3	60	40	100
4		Edge Computing Security (Sem VI)	3	0	0	0	3	60	40	100
5		Federated Learning Security (Sem VII)	3	0	0	0	3	60	40	100
6		Autonomous Systems Security (Sem VII)	3	0	0	0	3	60	40	100

L – Lecture, T – Tutorial, P – Practical, J – Project, C – No. of Credits, CIE – Continuous Internal Evaluation, SEE- Semester End Examinations, TM – Total Marks

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

APPLIED STATISTICS & STOCHASTIC PROCESSES [As per Choice Based Credit System (CBCS) scheme] **SEMESTER - III**				
Course Code	**:**		**Credits**	**:** 03
Hours / Week	**:** 03		**Total Hours**	**:** 45
L–T–P–J	**:** 3–0–0–0		**CIE+SEE**	60+40 Marks

Course Vision:

To develop strong foundations in probability, statistical inference, and stochastic process, enabling students to analyze uncertainty, make data-driven decisions, and explore advanced computational models including AI systems.

Course Objectives:

This course will enable students to:

1. **Understand** the concepts of random variables and probability distributions for modelling uncertainty.
2. **Analyze** relationships between variables using correlation and regression techniques.
3. **Apply** statistical inference methods for decision-making under uncertainty.
4. **Use** parametric and non-parametric tests for hypothesis testing and data analysis.
5. **Discuss** the fundamentals of stochastic processes and their applications in modeling random systems, decision-making, and AI-driven applications.

Teaching-Learning Process (General Instructions)

Following are sample new pedagogical methods, where teachers can use to accelerate the attainment of the various course outcomes:

1. Lecture Method**:** Concepts, algorithms, and models are explained through structured lectures supported by R Programming demonstrations.
2. Interactive Teaching**:** Active learning is promoted through discussions, brainstorming, and group problem-solving activities.
3. Demonstration using R Programming and Python**:** AI techniques like classification and optimization are demonstrated to visualize results and understand implementation.
4. Multimedia Learning: Videos and simulations are used to explain complex concepts and real-world applications.
5. Collaborative Learning: Students work in groups to implement projects and analyze datasets using computational tools.
6. Higher Order Thinking Questions: Analytical questions are used to develop model design, evaluation, and decision-making skills.
7. Problem-Based Learning: Real-world problems are given to apply techniques using Python

for practical solutions.

MODULE – I	**09 Hours**
Random Variables and Probability Distributions **Topics:** Introduction to random variables, probability mass function (PMF), probability density function (PDF), distribution functions, joint probability distribution and joint density functions, marginal and conditional distributions, mathematical expectation and its properties, covariance, moment generating function, characteristic function. **Applications:** Risk analysis and financial modelling, Reliability engineering, Data analysis and forecasting, Signal processing	
MODULE – II	**09 Hours**

Inference for Decision Making – I **Topics:** Introduction to hypothesis, hypothesis testing procedure, p-values and decision making, test of hypothesis for proportion (single and difference of proportions), testing hypothesis about mean (Z-test and t-test), two-sample tests, test for equality of variance (F-test), ANOVA (one-way analysis of variance). **Applications:** Quality assurance and control, Clinical trials and testing, Business decision- making, Industrial process evaluation	
MODULE – III	**09 Hours**
Inference for Decision Making – II **Topics:** Introduction to non-parametric tests, Chi-Square test for goodness of fit, Chi-Square test using probability distributions, Chi-Square test for independence of attributes, Run and rank test. **Applications:** Survey data analysis, Market research, Pattern recognition, Categorical data analysis.	
MODULE – IV	**09 Hours**
Bi-variate Data, Correlation and Regression Analysis **Topics:** Bi-variate random variables, correlation, types of correlation, measures of correlation, graphical methods (scatter diagram), Karl Pearson's correlation, rank correlation (for repeated and non-repeated ranks), linear regression model, regression lines, least squares method, fitted model. **Applications:** Market trend analysis, Economic forecasting, Quality control and process analysis, Data relationship analysis	
MODULE – V	**09 Hours**
Stochastic Processes **Topics:**Poisson Process, Introduction to Stochastic Processes (SPs), Markov chains, Discrete-time Markov Chains (DTMCs), Continuous-time Markov Chains (CTMCs), Monte-Carlo Simulation. **Applications:** Queueing systems and waiting line models, Reliability and maintenance systems, Population growth and epidemic modelling, Financial market analysis	

Authentic Intelligence:

1. Understanding uncertainty in AI predictions
2. Avoiding misleading interpretations of correlations
3. Interpreting statistical results responsibly
4. Ethical handling of categorical data
5. Ethical use of simulation-based decision models

AI Integration:

1. Feature distribution modelling in data science
2. Regression models in machine learning
3. Statistical decision-making in AI systems
4. Model validation using statistical tests
5. Markov models in reinforcement learning and decision processes

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Understand probability concepts and random variables to quantify uncertainty.	L3
2	Perform hypothesis testing and statistical inference for decision making.	L4
3	Apply non-parametric tests for categorical data analysis.	L4
4	Analyze data using correlation and regression techniques.	L3
5	Model and analyze stochastic processes such as Markov chains.	L5

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs													
	Program Outcomes (POs)											PSOs	
COS	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**1**	**2**
CO-1	3	2			2					1			
CO-2	3	3	2	2	3				1	1			
CO-3	3	3	3	2	3				1	2			
CO-4	3	2	2	2	2					1			
CO-5	3	3	2	3	3			1		1	2		

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Gupta, S. C., and V. K. Kapoor. Fundamentals of Applied Statistics. S. Chand, 2006.
2. Miller, Irwin, Marylees Miller, and John E. Freund. Miller and Freund's Probability and Statistics for Engineers. 8th ed., Pearson, 2018.
3. Mendenhall, William, Robert J. Beaver, and Barbara M. Beaver. Introduction to Probability and Statistics. Cengage Learning, 2020.
4. Ross, Sheldon M. Stochastic Processes. 2nd ed., John Wiley & Sons, 1995.
5. Operations Research: An Introduction Taha, Hamdy A. Operations Research: An Introduction. 10th ed., Pearson Education, 2017.

REFERENCE BOOKS:

1. R.E. Walpole, R.H. Mayers, S.L. Mayers and K.Ye, Probability and Statistics for engineers and scientists, 9th Edition, Pearson Education, 2018.
2. Douglas A. Wolfe, Grant Schneider, Intuitive Introductory Statistics, Springer, 2017.

3. Miller & Freund's, Probability and statistics for engineers, 8th edition, Pearson publication, 2018.
4. Richard I. Levin, David S. Rubin, Masood H. Siddiqui, Sanjay Rastogi, Statistics for Management, 8th Edition, Pearson Publications, 2018.
5. Mark L. Berenson, David M. Levine, Kathryn A. Szabat, Basic Business Statistics Concept and Application, Thirteenth Edition, Pearson Education Limited, 2015.
6. Bruce L. Bowerman, Richard T. O'Connell, Emily S. Murphree, Business Statistics in Practice, Seventh Edition, McGraw-Hill, 2014.
7. Douglas C. Montgomery, George C. Runger, Applied Statistics and Probability for Engineers, Sixth Edition, John Wiley and Sons, 2014.
8. Norean R. Sharpe, Richard D. De Veaux, Paul F. Velleman, Business Statistics, Fourth Edition, Pearson Education. 2019.

E-RESOURCES:

RECOMMENDED TOOLS

- Python
- R Programming

LAB EXERCISES

S. No	Exercise Title	Aim / Objective	Tools	Hrs	CO
MODULE I: Exercises 1–3: Random Variables and Probability Distributions (03 Hours)					
1	Random Variable Visualization	Generate and visualize discrete and continuous random variables	R Programming	1 h	CO1
2	PMF, PDF & CDF	Compute PMF, PDF, and CDF for standard distributions	R Programming	1 h	CO1

3	Joint Distributions	Simulate joint probability distributions	R Programming	1 h	CO1
MODULE II: Exercises 4–6: Bi-variate Data, Correlation and Regression Analysis (03 Hours)					
4	Bivariate Data Visualization	Visualize bivariate data using scatter plots	R Programming	1 h	CO2
5	Correlation Analysis	Compute Karl Pearson's and Spearman's rank correlation	R Programming	1 h	CO2
6	Linear Regression	Fit and evaluate regression model	R Programming	1 h	CO2
MODULE III: Exercises 7–9: Inference for Decision Making – I (03 Hours)					
7	Z-Test & t-Test	Perform Z-test and t-test (single & two-sample)	R Programming	1 h	CO3
8	Proportion Testing	Test for proportion and difference of proportions	R Programming	1 h	CO3
9	F-Test &	Perform F-test and one-way	R Programming	1 h	CO3

S. No	Exercise Title	Aim / Objective	Tools	Hrs	CO
	ANOVA	ANOVA			
MODULE IV: Exercises 10–12: Inference for Decision Making – II (03 Hours)					

10	Chi-Square Tests	Perform goodness of fit and independence tests	R Programming	1 h	CO 4
11	Bayesian Inference	Implement basic Bayesian inference techniques	R Programming	1 h	CO 4
12	Data Visualization	Visualize probability distributions and statistical results	R Programming	1 h	CO 4
MODULE V: Exercises 13–15: Stochastic Processes (03 Hours)					
13	Monte Carlo Simulation	Perform Monte Carlo simulations for probabilistic models	R Programming	1 h	CO 5
14	Markov Chains	Construct transition matrices and simulate state transitions	R Programming	1 h	CO 5
15	Exponential Distribution	Study exponential distribution and waiting time analysis	R Programming	1 h	CO 5

DATA STRUCTURES AND ALGORITHMS

[As per Choice Based Credit System (CBCS) Scheme]

SEMESTER – III

Course Code	:		Semester	:	3
Prerequisites	:	Introduction to C Programming	Hours / Week	:	5 Hours
Course Type	:	Core	Credits	:	04
L – T – P – J	:	3 – 0 – 2 – 0	Total Hours	:	45+15 Hours

Course Vision

The course on Data Structures and Algorithms aims to build a strong foundation in computational thinking and problem-solving by equipping students with essential techniques to design, analyse, and optimize algorithms. It focuses on understanding how data is organized, processed, and efficiently utilized to solve real-world problems.

Course Objectives

At the end of course students will be able to: To understand the fundamental concepts of algorithms, their characteristics, and performance evaluation using asymptotic notations. To impart knowledge on mathematical techniques to analyze both recursive and non-recursive algorithms, including solving recurrence relations. To familiarize the basic data structures such as arrays, linked lists, stacks, queues, and trees using C programming concepts. To impart the basic algorithm design techniques such as brute force, divide and conquer, greedy methods, dynamic programming, and backtracking to solve computational problems. To understand and compare different algorithms based on efficiency, scalability, and suitability for real-world applications.

MODULE – 1: Foundations of Algorithms	08 Hours

Algorithm Basics, Performance Analysis & Recurrence Relations

Topics: Algorithm: Definition and characteristics; Performance analysis and efficiency; Asymptotic notations: Big-O, Theta, Omega; Mathematical analysis of algorithms: Non-recursive and recursive algorithms; Recurrence relations: Substitution method, recursion tree method, Master theorem.

AI Integration & Authentic Intelligence Reflection (AI² Pedagogy):

AI Integration: Use USF Data Structure Visualizations to explore algorithm performance visually: https://www.cs.usfca.edu/~galles/visualization/Algorithms.html

Authentic Intelligence Reflection: Reflect on how asymptotic notation helps in making design decisions; critically evaluate the efficiency of a chosen algorithm using Big-O analysis.

MODULE – 2: Basic Data Structures	10 Hours

Arrays, Pointers, Linked Lists & Divide and Conquer

Topics: Introduction to Arrays, Pointers and dynamic memory allocation; Divide and Conquer — merge sort and quick sort; Linked lists: Singly and doubly linked lists; operations including insertion, deletion, and traversal; Circular linked list.

AI Integration & Authentic Intelligence Reflection (AI² Pedagogy):

AI Integration: USF Data Structure Visualizations — linked list module: https://www.cs.usfca.edu/~galles/visualization/Algorithms.html

Authentic Intelligence Reflection: In module 2 the visualization tools are used to verify understanding of the core concept that includes linked list. The visualization tools act as a powerful feedback mechanism to enhance learning. By leveraging such tools, learners can experience adaptive feedback for continuous improvement.

MODULE – 3: Stacks, Queues, and Trees	08 Hours

Stacks, Queues, Expression Evaluation & Tree Structures

Topics: Stacks: Linked list implementation; Queues: Linear queue; linked list implementation; Expression evaluation using stacks; Trees: Binary trees, representation, and traversal techniques; Binary Search Trees (BST): Operations; Balanced trees: AVL trees.

AI Integration & Authentic Intelligence Reflection (AI² Pedagogy):

AI Integration: USF Data Structure Visualizations — stack, queue, and tree modules: https://www.cs.usfca.edu/~galles/visualization/Algorithms.html

Authentic Intelligence Reflection: In module 3 the visualization tools are used to verify understanding of the core concepts that includes stack, queue and trees. The visualization tools act as a powerful feedback mechanism to enhance learning. By leveraging such tools, learners can experience adaptive feedback for continuous improvement.

MODULE – 4: Algorithm Design Techniques	09 Hours

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

Brute Force, Graph Traversal & Hashing

Topics: Brute force techniques: String matching; Graph representations: adjacency list, matrix; Graph traversal algorithms: Depth First Search (DFS), Breadth First Search (BFS), Dijkstra's algorithm; Hashing: Open and closed hashing techniques.

AI Integration & Authentic Intelligence Reflection (AI² Pedagogy):

AI Integration: USF Data Structure Visualizations — graph and hashing modules: https://www.cs.usfca.edu/~galles/visualization/Algorithms.html

Authentic Intelligence Reflection: In module 4 the visualization tools are used to verify understanding of the core concepts that includes graphs. The visualization tools act as a powerful feedback mechanism to enhance learning. By leveraging such tools, learners can experience adaptive feedback for continuous improvement.

MODULE – 5: Advanced Algorithms	10 Hours

Greedy Methods, Dynamic Programming & Backtracking

Topics: Greedy algorithms: Fractional knapsack problem; Minimum Spanning Trees: Prim's and Kruskal's algorithms; Dynamic programming: Concept and methodology; 0/1 knapsack problem and Floyd-Warshall algorithm; Backtracking: Concept and methodology; Sum of Subsets problem; P, NP, NP Hard, NP Complete.

AI Integration & Authentic Intelligence Reflection (AI² Pedagogy):

AI Integration: USF Data Structure Visualizations — algorithm design modules: https://www.cs.usfca.edu/~galles/visualization/Algorithms.html

Authentic Intelligence Reflection: Reflect on the trade-offs between greedy and dynamic programming approaches for the knapsack problem; critically evaluate when backtracking is a practical choice vs. other design strategies.

CO	Course Outcome	Blooms Level
CO1	Analyze the efficiency of algorithms using asymptotic notations, recurrence relations, and mathematical techniques to evaluate computational complexity.	L4
CO2	Implement linear data structures such as arrays, linked lists, stacks, and queues to solve computational problems efficiently.	**L3**
CO3	Apply tree-based data structures and traversal algorithms to organize, search, and process hierarchical data.	**L3**
CO4	Identify solutions using fundamental algorithm design techniques including divide-and-conquer, graph traversal, hashing, and brute-force approaches.	**L3**
CO5	**I**mplement advanced algorithmic strategies such as greedy methods, dynamic programming, and backtracking to solve optimization and decision problems while distinguishing complexity classes (P, NP, NP-Hard, NP-Complete).	**L3**

COs \ POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	3	3	1	2	1	-	-	-	-	-	-	3	2
CO2	3	2	3	2	3	-	-	-	1	-	-	3	2
CO3	3	3	3	2	3	-	-	-	1	-	-	3	2
CO4	3	3	3	3	3	-	-	-	1	-	-	3	2
CO5	3	3	3	3	2	-	-	-	1	-	-	3	2

Text Books

1. **Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein**, *Introduction to Algorithms*, 4th Edition, MIT Press, 2022.
2. **Ellis Horowitz, Sartaj Sahni, and Dinesh Mehta**, *Fundamentals of Data Structures in C++*, 2nd Edition, Universities Press.

Reference Books

1. **Mark Allen Weiss**, *Data Structures and Algorithm Analysis in C++*, 4th Edition, Pearson Education.
2. **Alfred V. Aho, John E. Hopcroft, Jeffrey D. Ullman**, *Data Structures and Algorithms*, Addison-Wesley.
3. **Robert Sedgewick and Kevin Wayne**, *Algorithms*, 4th Edition, Addison-Wesley.
4. **Steven S. Skiena**, *The Algorithm Design Manual*, 3rd Edition, Springer.
5. **S. Dasgupta, C. Papadimitriou, U. Vazirani**, *Algorithms*, McGraw-Hill Education.

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

DATA STRUCTURES LABORATORY

Total Contact Hours: 30 Hours

Following are experiments to be carried out using either C programming language.

1. To Implement C programs to perform array operations.
2. To determine the validity of a 9x9 Sudoku board (application of 2-dimensional array).
3. To store, retrieve and update the elements in structures (structures and pointers to structures).
4. To implement stack using linked list.
5. To implement a queue data structure using a singly linked list.
6. To implement a singly linked list and its operations.
7. To implement a doubly linked list and its operations.
8. To create a circular queue using a circular linked list data structure
9. To implement binary tree traversal techniques.

OPEN-ENDED EXPERIMENTS

1. Design a web browser history tracker in C. Implement a stack data structure to keep track of visited URLs. Create functions to push new URLs onto the stack as users visit websites and pop URLs when users navigate backward in their browsing history.
2. Imagine you are responsible for designing a queue-based system to manage the queue of regular customers waiting to purchase cinema tickets at a popular movie theatre. Your system should ensure fair and efficient ticket sales for all customers. When a customer's arrive at the cinema, they join the queue. Each customer is represented by his name, age (for record-keeping), and number of tickets needed. When a customer reaches the front of the queue, they are served by the ticketing agent. Implement a ticket sale process where the agent provides the customer with the requested ticket(s). Initialize the total number of tickets and if the tickets are sold, then the ticketing agent should display a houseful message.

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

Digital Logic and Computer Organization

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER -III

Course Code	**:**		**Credits**	**:**	03
Hours / Week	**:**	3	**Total Hours**	**:**	45
L–T–P–J	**:**	3–0–0–0	**CIE+SEE**	**:**	60+40 Marks

Course Vision:

To provide a strong foundation in digital logic and computer organization, enabling students to understand, design, and analyze modern computing systems, while developing problem-solving skills and the ability to apply core concepts in real-world hardware and system-level applications.

Course Objectives:

This course will enable students:

1. **To introduce** the fundamentals of Verilog HDL, including syntax, operators, and coding structure.

2. **To provide** a foundation for advanced studies in VLSI design, embedded systems, processor architecture, and intelligent digital hardware systems.

3. **To understand** the fundamentals of sequential circuits including latches, gated latches, and various types of flip-flops such as SR, D, JK, T, and master-slave JK flip-flops.

4. **To understand** the principles and organization of cache memory and its role in improving processor performance.

5. **To study** different instruction formats and addressing modes used in computer architecture for efficient data access and execution.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with traditional lecture method, different types of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I	**09 Hours**

INTRODUCTION:

Topics: Number System- Binary, Hexa, Decimal, Octal and its conversion. Canonical Notation - SOP & POS forms, Minimization of SOP and POS forms.

ARITHMETIC CIRCUITS AND VERILOG MODELLING

Adders: Half adder, full adder, Ripple carry adder, parallel adder /subtractor, fast adders-CLA, comparator- 2 bit. Simplification using K-Maps , Introduction to Verilog, Syntax of Verilog coding, Modelling styles in Verilog, Verilog Operators, Test bench for simulation.

Applications:

- Used in computers and digital electronics for data representation.
- Hexadecimal numbers are used in memory addressing and programming.
- Binary conversions are essential in communication and embedded systems.

AI Integration:

- AI automatically generates test benches.
- Machine learning detects hardware bugs quickly.
- AI improves testing accuracy and speed.
- Used in smart semiconductor testing platforms.

Authentic Intelligence:

- AI optimizes digital circuit design and Boolean simplification.
- Used in intelligent chip design and FPGA development.
- AI-assisted tools automatically generate Verilog code.
- Helps in automatic testing and hardware verification.

MODULE – II	**09 Hours**

Combinational Circuit Building

Topics : Combinational Circuit Building: Multiplexers 4:1, 8:1, decoders 3:8, 2:4, demultiplexers 1:4, encoders 8:3, 4:2, code converters- B to G and G to B- Simplification using K-Maps , Verilog for combinational circuits,: if else, case-casex, casez, for loop, generate.

Applications:

- Used in Arithmetic Logic Units (ALU) for arithmetic and logical operations.
- Used in data routing through multiplexers and demultiplexers.
- Used in memory address decoding in computer systems.
- Used in communication systems for encoding and decoding data.

AI Integration:

- AI helps in automatic logic simplification and circuit optimization.
- Machine learning techniques improve fault detection in digital circuits.
- AI tools assist in Verilog code generation and hardware testing.
- AI reduces power consumption and improves FPGA routing efficiency.

Authentic Intelligence:

- Authentic Intelligence combines human intelligence with AI systems.
- It ensures ethical and transparent decision-making in technology.
- Human engineers verify AI-generated circuit designs for reliability.
- It improves trust, safety, and accuracy in digital system development.

MODULE – III	**09 Hours**

Sequential Circuits-1

Topics:

Sequential Circuits-1

Basic Latch, Gated latches, Flip Flops SR, D, JK, T, master-slave flip-flops JK, Characteristic equations, 0's and 1's Catching Problem, race round condition, Switch debounce, shift registers- SISO, SIPO, PISO, PIPO, Setup time, Hold time, Propagation Delay.

Applications:

- Used in memory storage elements and processor registers.
- Shift registers are used in serial and parallel data communication.
- Flip-flops are widely used in counters, timers, and control systems.
- Setup time, hold time, and propagation delay are important in high-speed processor and embedded system design.

AI Integration:

- AI processors use flip-flops and registers for temporary data storage.
- Shift registers support fast data transfer in neural network hardware.
- Sequential circuits enable AI pipeline processing and synchronization.
- AI-based embedded systems use timing analysis for reliable computation.

Authentic Intelligence:

- Sequential circuits support real-time intelligent decision-making systems.
- Flip-flops store intermediate states in intelligent hardware systems.
- Timing parameters ensure accurate and reliable intelligent computation.
- Race condition prevention improves trustworthy AI hardware operations.

MODULE – IV	**09 Hours**

Computer Memory:

Topics: Cache memory principles-Elements of Cache Design-Internal Memory: Semiconductor Main Memory-Advanced DRAM Organization-External Memory: Magnetic Disk-RAID-SSD-Optical memory.

Applications:

- Increases processor performance by reducing memory access time
- Used in modern CPUs and GPUs for fast computation
- Supports multitasking and high-speed applications
- Improves execution speed in operating systems and databases

AI Integration:

- Cache memory accelerates AI model execution and inference.
- DRAM supports high-speed training of machine learning models.
- SSDs improve AI dataset loading and processing performance.
- RAID systems provide reliable storage for large-scale AI data.

Authentic Intelligence :

- Intelligent systems require fast and reliable memory access mechanisms.
- Cache and DRAM improve real-time intelligent decision-making.
- RAID and SSD ensure secure and trustworthy intelligent data storage.

MODULE – V	**09 Hours**

Instruction Sets and CPU :

Topics: Characteristics and Functions - Instruction Sets: Addressing Modes and Formats - Processor Structure and Function: Processor Organization-Register Organization-Instruction Cycle- Instruction Pipelining-Arithmetic Pipelining – Control Unit Operation- RISC- CISC. **Input/output External Devices:** I/O modules - Programmed I/O – Interrupts – Interrupt-driven I/O – Direct Memory Access – I/O Channels – External Interface.

Applications:

- Controls processor operations and execution flow
- Supports communication between hardware and software
- Used in operating systems and embedded systems
- Essential for assembly language programming

AI Integration:

- Instruction pipelining improves AI computation speed and efficiency.
- DMA enables fast transfer of large AI datasets.
- RISC processors are widely used in AI-enabled embedded systems.
- Interrupt-driven I/O supports real-time AI and robotic applications.

Authentic Intelligence:

- Intelligent systems require efficient instruction execution and data transfer.
- Pipelining supports real-time intelligent decision-making systems.
- DMA and interrupts improve responsive intelligent computing environments.
- RISC and CISC architectures support reliable AI and embedded applications.

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Understand the fundamentals of Verilog HDL, including syntax, operators, and modelling styles.	L2
2	Understand the operation and applications of multiplexers, decoders, encoders, and demultiplexers in digital systems.	L2
3	Apply sequential circuit concepts in counters, registers, communication systems, and processor design.	L3
4	Explain the principles and organization of cache memory and its role in improving computer system performance.	L2
5	Apply processor and I/O organization concepts in embedded systems, high-performance computing, cyber security, and intelligent computing applications.	L3

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

	Program Outcomes (POs)											PSOs	
COs	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**1**	**2**
CO1	2	1	2	2	3	1			2	2		2	2
CO2	2	1	2	2	3	1			2	2		2	2
CO3	2	1	2	2	3	1			2	2		2	2
CO4	2	1	2	2	3	1			2	2		2	2
CO5	2	1	2	2	3	1			2	2		2	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. M. Morris Mano, Michael D. Ciletti , "Digital Design with an Introduction to the Verilog HDL", 6th Edition, Pearson Education, 2014.

2. Stephen Brown, Zvonko Vranesic, "Fundamentals of Digital Logic with Verilog design", McGraw Hill, 2014.

3. William Hohl, "ARM Assembly Language," 2nd Edition, CRC Press, 2009.

4. John L. Hennessy, David A. Patterson, "Computer Architecture: A Quantitative Approach",5th Edition, Morgan Kaufmann Publishers, 2012.

REFERENCE BOOKS:

1.John M Yarbrough, "Digital Logic Applications and Design", Thomson Learning, 2014.

2.Donald D. Givone, "Digital Principles and Design", McGraw Hill, 2015.

3.Samir Palnitkar, "Verilog HDL: A Guide to Digital Design and Synthesis", Pearson Education, 2016.

4.David A Patterson, John L Hennessy, "Computer Organization and Design", 4th Edition, Morgan Kaufmann publishers, 2010.

E-Resources:

https://archive.nptel.ac.in/courses/106/105/106105165/

https://nptel.ac.in/courses/117105080

Recommended Tools

- Digital Logic Design & Simulation
- HDL Design & Simulation Tools
- FPGA & Hardware Implementation
- Processor & Architecture Simulation

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

COMPUTER NETWORKS

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - III

Course Code	:		**Credits**	:	04
Hours / Week	:	05	**Total Hours**	:	45+30
L–T–P–J	:	3–0–2–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

To empower students with the knowledge and skills required to understand, design, analyze, and implement computer networks, enabling them to address real-world communication challenges using modern tools and technologies.

Course Objectives:

This course will enable students:

1. Understand layered network architecture and communication models.
2. Analyze data transmission and error control mechanisms
3. Design routing and IP addressing schemes
4. Evaluate transport protocols and congestion control
5. Explore application layer protocols and real-world networking

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with traditional lecture method, different types of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I	**09 Hours**

Introduction: Data Communications, Networks, Network Types, Network Models, Protocol Layering, Reference Models: The OSI Reference Model, The TCP/IP Reference Model, Physical Layer: Data and signals Digital Transmission, (D-D Conversion) Bandwidth Utilization, Multiplexing, Switching, Circuit Switched Networks, Packet Switching.

Applications: Internet backbone, Telecom systems

AI Integration: Wireshark, Cisco Packet Tracer

Authentic Intelligence: Analyze latency differences in switching

MODULE – II	**09 Hours**

Data Link Layer: Link Layer Addressing, Error Detection and Correction, Block Coding, Cyclic Codes, Checksum. Data Link Control: DLC Services, Data-Link Layer Protocols, Media Access Control, Wired LANs, Ethernet protocol.

Applications: LAN networks, Ethernet communication.

AI Integration: NS2/NS3, MATLAB

Authentic Intelligence: Study packet loss and retransmissions

MODULE – III	**09 Hours**

Network Layer: Network Layer Services, Packet Switching, Network Layer Performance, IPV4 Addresses. Network Layer Protocols: Internet Protocol, ICMPV4, Unicast Routing, Routing algorithms, Unicast routing protocols, Internet Structure, Routing Information Protocol (RIP), Next Generation IP: IPV6 Addressing, IPV6 Protocol, ICMPv6 Protocol, Transition from IPV4 to IPV6, Congestion Control Algorithms, QoS.

Applications: Internet routing, Cloud networking

AI Integration: Cisco Packet Tracer, Python

Authentic Intelligence: Case study on congestion

MODULE – IV	**09 Hours**

Introduction and Transport-Layer Services: Overview of the Transport Layer in the Internet,: Connectionless Transport: UDP, UDP Segment Structure, UDP Checksum, Principles of Reliable Data Transfer: Building a Reliable Data Transfer Protocol, Pipelined Reliable Data Transfer Protocols: Go-Back-N, Selective repeat, Connection-Oriented Transport TCP: The TCP Connection, TCP Segment Structure, Reliable Data Transfer, Flow Control, TCP Connection Management, Principles of Congestion Control: The Causes and the Costs of Congestion, Approaches to Congestion Control.

Applications: Streaming services, Online applications

AI Integration: Wireshark, Socket programming

Authentic Intelligence: Compare TCP vs UDP performance

MODULE – V	**09 Hours**

Application Layer: Introduction, client server programming, WWW (World Wide Web) and HTTP (Hyper Text Transfer Protocol), FTP (File Transfer Protocol), E-mail, telnet, DNS (Domain Naming System) SNMP (Simple Network Management Protocol).

Applications: Web systems, Email services

AI Integration: Postman, MQTT tools

Authentic Intelligence: Build client-server application

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Explain network models and physical layer transmission techniques.	L2, L3
2	Analyze error control techniques and data link layer protocols.	L3, L4
3	Design IP addressing and evaluate routing algorithms.	L3, L4, L5
4	Evaluate transport layer protocols and congestion mechanisms.	L3, L4, L5
5	Analyze application layer protocols and services.	L3, L4

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs													
COs	**Program Outcomes (POs)**											**PSOs**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**1**	**2**
CO1	**3**	**2**	**-**	**-**	**2**	**-**	**-**	**-**	**-**	**-**	**1**	**2**	**-**
CO2	**3**	**3**	**2**	**1**	**2**	**-**	**-**	**-**	**-**	**-**	**2**	**2**	**-**
CO3	**3**	**3**	**3**	**2**	**2**	**-**	**-**	**-**	**-**	**-**	**3**	**3**	**-**
CO4	**3**	**3**	**2**	**2**	**2**	**-**	**-**	**-**	**-**	**-**	**3**	**3**	**-**
CO5	**3**	**2**	**2**	**1**	**2**	**-**	**-**	**-**	**-**	**-**	**2**	**2**	**2**

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Behrouz A. Forouzan—Data Communications and Networking‖, TataMcGraw-Hill,5th Edition, 2012.
2. Andrew S. Tanenbaum, David.J.Wetherall, —Computer Networks‖, Prentice-Hall, 5th Edition 2010.
3. James F Kurose and Keith W Ross, Computer Networking, A Top-Down Approach, Sixth edition, Pearson, 2017.

REFERENCE BOOKS:

1. Data and Computer Communication William Stallings 8th Edition Pearson Education 2008.
2. Computer Networks – A Systems Approach Larry L. Peterson and Bruce S. Davie 4th Edition Elsevier 2007

E-BOOKS:

1. An Introduction to Computer Networks Peter L Dordal 1st Edition - 2020
https://intronetworks.cs.luc.edu/current/ComputerNetworks.pdf

2. A Top-Down Approach: Computer Networking James F Kurose & Keith W Ross

8th Edition Pearson

https://gaia.cs.umass.edu/kurose_ross/online_lectures.htm

LAB EXERCISES -30 Hours

S.No	Exercise Title	Aim / Objective	Tools	Hrs	CO
1	Ring Topology and Bus Topology	Implement Ring topology and Bus topology operation using NS2.	NS2/NS3	2 h	CO1
2	Three node point to point network	Implement three nodes point – to – point networks with duplex links between them. Set the queue size, vary the bandwidth and find the number of packets dropped.	NS2/NS3	2 h	CO1
3	Ethernet LAN using n-nodes with multiple traffic	Implement an Ethernet LAN using n nodes and set multiple traffic nodes and plot congestion window for different source /destination.	NS2/NS3	2 h	CO1
4	Simple ESS with wireless LAN	Implement simple ESS and transmitting nodes in wireless LAN by simulation and determine the performance with respect to transmission of packets.	NS2/NS3	2 h	CO2
5	Operation of Stop and wait Protocol	Write a NS2 script to implement the operation of Stop and Wait protocol	NS2/NS3	2 h	CO4
6	Error detection using CRC-CCITT	Write a program for error detecting code using CRC-CCITT (16-bits).	C, C++, Java, Python	2 h	CO2
7	Determination of shortest path using Bellman-Ford algorithm	Write a program to find the shortest path between vertices using Bellman-Ford algorithm.	C, C++, Java, Python	2 h	CO3
8	Congestion control using Leaky bucket concept	Write a program for congestion control using leaky bucket algorithm.	C, C++, Java, Python	2 h	CO3
9	Client/ Server Communication using TCP/ IP Socket	Write a program to Implement TCP/IP sockets, write a client – server program to make the client send the file name and to make the server send back the contents of the requested file if present	C, C++, Java, Python	2 h	CO4

S.No	Exercise Title	Aim / Objective	Tools	Hrs	CO
10	DNS Server	Implement a simple DNS server to resolve the IP address for the given domain name	C, C++, Java, Python	2 h	CO5

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

CYBER SECURITY ESSENTIALS

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - III

Course Code	:		**Credits**	:	03
Hours / Week	:	03	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

To develop foundational and applied competencies in cybersecurity, enabling learners to understand, analyze, and mitigate cyber threats using modern tools, ethical practices, and intelligent technologies.

Course Objectives:

The course aims to enable students to:

1. To introduce core principles of cybersecurity and threat landscape
2. To develop skills in securing systems, networks, and applications
3. To provide exposure to cyber laws, risk management, and ethical practices
4. To integrate AI-driven security approaches and authentic intelligence analysis
5. To prepare students for real-world cybersecurity problem-solving

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with traditional lecture method, different types of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I	**09 Hours**

FUNDAMENTALS OF CYBER SECURITY

Topics: Fundamentals of Cyber Security: CIA Triad (Confidentiality, Integrity, Availability), Cyber Security Terminology and Concepts, Types of Cyber Threats: Malware (Virus, Worm, Trojan, Ransomware, Spyware), Phishing and Social Engineering Attacks, Insider Threats and Advanced Persistent Threats (APT), Attack Vectors and Surfaces, Cyber Kill Chain Model.

Applications: Enterprise Security Awareness Programs, Threat Modelling in Organizations, Incident Response Planning

AI Integration: AI-based phishing detection tools, Malware classification using ML models, Threat intelligence platforms (AI-assisted SIEM)

Authentic Intelligence: Human intuition in identifying social engineering, Analyst-driven threat interpretation beyond automated alerts, Ethical decision-making in cyber defense

MODULE – II	**09 Hours**

NETWORK SECURITY

Topics: Network Security Architecture and Security Concepts, OSI & TCP/IP Security Issues , Common Network Attacks: DoS/DDoS, Man-in-the-Middle (MITM) , Packet Sniffing & Spoofing, Firewalls: Types (Packet Filtering, Stateful, Proxy), Intrusion Detection and Prevention Systems (IDS/IPS), Virtual Private Networks (VPNs), Wireless Network Security (WEP, WPA, WPA3).

Applications: Secure Network Design, Enterprise Firewall Configuration, Network Traffic Monitoring

AI Integration: AI-based intrusion detection systems, Network anomaly detection using ML, Automated log analysis tools

Authentic Intelligence: Human validation of anomaly detection results, Context-aware network defense strategies, Combining intuition with AI alerts

MODULE – III	**09 Hours**

CRYPTOGRAPHY & DATA SECURITY

Topics: Introduction to Cryptography, Symmetric Encryption (AES, DES), Asymmetric Encryption (RSA), Hash Functions (SHA family, MD5 limitations), Digital Signatures and Certificates, Basics of Public Key Infrastructure (PKI), Key Management and Distribution, Basics of Blockchain Security.

Applications: Secure Communication Systems, Digital Transactions and E-Commerce, Data Integrity Verification

AI Integration: AI-assisted cryptanalysis research tools, Blockchain analytics tools, Automated certificate management systems

Authentic Intelligence: Understanding limitations of encryption, Ethical considerations in cryptographic use, Human oversight in key management

MODULE – IV	**09 Hours**

SYSTEM SECURITY & RISK MANAGEMENT

Topics: Operating System Security: Access Control Models (DAC, MAC, RBAC), Vulnerability Assessment and Penetration Testing (VAPT), Malware Analysis Basics, Risk Management: Risk Identification, Assessment, Mitigation, Security Policies and Governance, Backup and Disaster Recovery, Security Auditing. **Applications:** Enterprise Risk Management, Security Audits and Compliance, Incident Handling **AI Integration:** AI-based vulnerability scanners, Automated penetration testing tools, Risk prediction models **Authentic Intelligence:** Human judgment in risk prioritization, Ethical hacking decision-making, Interpretation of automated scan results	
MODULE – V	**09 Hours**
Cyber Laws, Ethics **Topics:** Cyber Laws: Information Technology Act, 2000, Data Protection and Privacy Laws, Cyber Ethics and Professional Responsibility, Digital Forensics Basics, Emerging Trends: Cloud Security, IoT Security, AI in Cybersecurity, Zero Trust Architecture, Cyber Warfare and National Security **Applications:** Legal Compliance in Organizations, Digital Forensic Investigations, Secure Cloud Deployment. **AI Integration:** AI-based forensic tools, Cloud security posture management tools, Threat intelligence platforms **Authentic Intelligence:** Ethical reasoning in cyber investigations, Human-led forensic interpretation, Balancing automation with accountability	

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	**Understand** the core cybersecurity concepts, security principles (CIA triad), types of cyber threats, and basic cryptographic techniques for protecting information systems.	L3
2	**Apply** network security mechanisms such as firewalls, IDS/IPS, VPNs, and secure protocols to protect data communication and defend against network-based attacks.	L3
3	**Analyze** system and application vulnerabilities, including operating system weaknesses and web application threats (e.g., OWASP Top 10), and recommend appropriate mitigation strategies.	L4
4	**Interpret** cyber laws, ethical practices, and risk management frameworks to ensure legal compliance and develop incident response strategies.	L3

5	**Evaluate** emerging cybersecurity technologies such as cloud security, IoT security, AI in cybersecurity, and Zero Trust models to address modern threat landscapes.	L4

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	3	2	-	-	-	-	-	2	-	-	2	2	1
CO2	3	3	2	2	3	-	-	-	1	-	2	3	3
CO3	3	2	2	-	2	-	-	-	-	-	2	3	2
CO4	3	3	2	3	3	2	-	-	1	-	3	3	3
CO5	2	2	-	-	-	3	2	3	-	2	2	2	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Cybersecurity Essentials, Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short, 1st Edition, Cisco Press (Pearson Education), 2018, ISBN: 978-1587134388
2. Introduction to Cyber Security, The Open University, OpenLearn / The Open University.

REFERENCE BOOKS:

1. William Stallings, Lawrie Brown, Computer Security: Principles and Practice, 4th Edition, Pearson, 2018, ISBN: 978-0134794105.
2. William Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson, 2017, ISBN: 978-0134444284.
3. Dafydd Stuttard, Marcus Pinto, The Web Application Hacker's Handbook, 2nd Edition, Wiley, 2011, ISBN: 978-1118026472.
4. Jon Erickson, Hacking: The Art of Exploitation, 2nd Edition, No Starch Press, 2008, ISBN: 978-1593271442.

RECOMMENDED TOOLS

- Security Tools: Wireshark, Nmap, Metasploit, Burp Suite
- SIEM Tools: Splunk, IBM QRadar
- AI/ML Tools: Python (Scikit-learn, TensorFlow), Weka

- Cloud Security: AWS Security Hub, Azure Defender

Sustainability Engineering & Environmental Social and Governance (CSE Cluster)

Course Code:

Semester: 3rd

Programs Offered: B. Tech. (Common to all CSE Branches)

Prerequisites: Fundamental understanding of engineering mathematics, Basic awareness of environmental science

Course Type: Core

L – T – P – J: 2 – 0 – 0 – 0 *(2 Credits Theory)*

Course Vision

This course aims to develop a strong foundation in sustainable engineering, Environmental, Social, and Governance (ESG) principles, and digital sustainability systems, enabling students to analyse and address real-world challenges related to energy efficiency, environmental impact, ethical computing, and sustainable digital infrastructure. The course integrates modern analytical tools, AI-based decision-making, and data-driven sustainability assessment methods to enhance problem-solving and critical thinking.

Course Objectives

Students will:

1. Understand the fundamental concepts of sustainable engineering, ESG framework, and environmental, social, and governance dimensions of digital and computing systems, including energy usage and environmental impact.
2. Apply sustainability principles, ESG indicators, and basic analytical models to assess environmental performance and resource efficiency in engineering and digital systems.
3. Analyse energy consumption patterns, system efficiency, and environmental impacts in computing infrastructures such as data centers, cloud systems, and software applications.
4. Understand sustainability metrics, lifecycle assessment concepts, and ethical considerations in engineering systems, including responsible use of digital technologies.
5. Evaluate the performance of engineering and digital systems in terms of energy efficiency, sustainability impact, and alignment with ESG goals, using modern analytical and AI-assisted tools.

Course Outcomes (CO)

CO	Outcome
CO1	Explain fundamental concepts of sustainability engineering, ESG framework, and analyse environmental impact factors such as energy consumption and resource usage in digital systems.
CO2	Apply sustainability principles, ESG indicators, and analytical models to evaluate environmental performance and efficiency in computing and engineering systems.

CO	Outcome
CO3	Evaluate energy usage patterns, system efficiency, and resource optimization in IT infrastructure such as cloud systems, data centers, and software applications.
CO4	Analyse sustainability metrics and lifecycle impacts of engineering systems using ESG reporting frameworks, carbon footprint estimation, and responsible design principles.
CO5	Apply sustainability and ESG principles to assess the performance of digital systems in terms of energy efficiency, environmental impact, and ethical governance using AI-assisted tools.

Broad Course Description

Sustainable Engineering and Environmental Governance is an integrated course that introduces the fundamental principles of sustainability science, environmental impact assessment, and ESG (Environmental, Social, and Governance) frameworks to analyse and design responsible digital and engineering systems. The course begins with an understanding of sustainability concepts, ESG principles, and global sustainability goals (SDGs), followed by the evaluation of environmental impacts of computing and engineering systems such as energy consumption, carbon footprint, and resource utilization.

Key topics include green computing, lifecycle assessment (LCA), energy efficiency in IT infrastructure, and sustainable system design, with emphasis on applications in cloud computing, data centers, software systems, and smart infrastructure. The course also explores social and ethical dimensions of technology, including digital inclusivity, data privacy, ethical AI, and algorithmic fairness.

The governance aspect introduces ESG reporting frameworks, sustainability metrics, and compliance standards, enabling students to assess and communicate sustainability performance effectively. AI-based tools are integrated throughout the course for sustainability analytics, carbon estimation, ESG reporting, and energy optimization, enhancing data-driven decision-making.

The course combines theoretical concepts with case studies, AI-assisted analysis, and project-based learning, enabling students to develop analytical skills and responsible engineering judgment required to design and evaluate sustainable digital systems in industries such as IT services, cloud computing, smart cities, and emerging green technologies.

Detailed Course Syllabus

The course consists of five modules. Each module integrates:

- Core topics
- Engineering applications
- AI integration
- Authentic Intelligence reflection

Course Modules

Module 1: Sustainability Fundamentals & ESG

Topics: Sustainable development, Triple Bottom Line, ESG framework, SDGs, ESG vs CSR, sustainability challenges in digital economy.

Engineering Applications: Green computing, sustainable IT infrastructure, energy-efficient data centers.

AI Integration: AI-based sustainability trend analysis, ESG scoring tools.

Module 2: Environmental Sustainability in Digital Systems

Topics: Carbon footprint of IT systems, energy consumption in data centers, lifecycle assessment (LCA), e-waste management, green cloud computing.

Engineering Applications: Energy-efficient servers, cloud optimization, sustainable software engineering.

AI Integration: AI models for energy prediction and carbon footprint estimation.

MODULE 3: Social Sustainability & Ethical Computing

Topics: Stakeholder analysis, digital inclusivity, data privacy, ethical AI, cybersecurity and society, social impact of automation.

Engineering Applications: AI ethics in recommendation systems, fairness in algorithms, inclusive software design.

AI Integration: Sentiment analysis, bias detection in AI systems.

Module 4: Governance, ESG Reporting, Sustainable Design & Future Technologies

Topics: Corporate governance, ESG reporting frameworks (GRI, TCFD), ESG metrics, sustainability KPIs, data visualization, Circular economy, sustainable software design, green AI, smart cities, Industry 4.0 sustainability, digital twins for sustainability

Engineering Applications: Corporate ESG dashboards, compliance analytics, risk management systems, Smart grids, intelligent transportation, sustainable IoT systems.

AI Integration: AI-based ESG report analysis, dashboards using Power BI/Python, AI-based optimization of sustainable systems.

Module 5: Energy Efficiency, Audit & Smart Energy Systems

Topics: Energy efficiency metrics, Energy losses in computing and electronic systems, Energy-efficient computing: green computing principles, low-power design, Energy Audit: types (preliminary and detailed audit), steps involved, Energy audit of IT infrastructure, Introduction to smart energy management systems

Engineering Applications: Energy-efficient data centers and cloud computing systems, Power optimization in embedded systems and IoT devices, Energy audit of IT infrastructure in industries and campuses

AI Integration: AI-based energy consumption prediction using machine learning models, Optimization of energy usage in data centers using AI algorithms.

AI Integration & Authentic Intelligence Reflection (AI² Pedagogy)

- **AI Integration:**
  - **Module 1 — Sustainability Fundamentals & ESG**
    - Use AI tools for sustainability trend analysis and ESG scoring based on real-world datasets.
    - AI-based visualization of SDGs, ESG indicators, and sustainability performance metrics for organizations.
  - **Module 2 — Environmental Sustainability in Digital Systems**
    - AI-assisted estimation of carbon footprint and energy consumption in IT systems and data centers.
    - Machine learning models for energy prediction, workload optimization, and green cloud computing strategies.
  - **Module 3 — Social Sustainability & Ethical Computing**
    - AI tools for sentiment analysis and stakeholder impact assessment.
    - AI-based detection of bias, fairness issues, and ethical concerns in algorithms and digital systems.
  - **Module 4 — Governance, ESG Reporting, Sustainable Design & Future Technologies**
    - AI-assisted ESG report analysis, KPI tracking, and sustainability dashboards (Power BI/Python tools).
    - AI-based optimization of smart cities, digital twins, Industry 4.0 systems, and sustainable IoT infrastructures.
  - **Module 5 — Energy Efficiency, Audit & Smart Energy Systems**
    - AI models for energy consumption prediction and anomaly detection in IT infrastructure.
    - AI-based optimization of data center energy usage, smart energy monitoring using IoT, and identification of energy loss points.

- **Authentic Intelligence Reflection:**
  - **Module 1**: Students critically evaluate AI-generated ESG scores, sustainability indicators, and SDG mappings, identifying inconsistencies, data gaps, and assumptions in AI-based assessments.
  - **Module 2:** Students verify AI-based predictions of carbon footprint and energy consumption in IT systems, assessing limitations in datasets, boundary conditions, and real-world applicability.
  - **Module 3:** Students analyse AI outputs for bias detection, fairness, and ethical implications, identifying potential risks in algorithmic decision-making and digital inclusivity.
  - **Module 4:** Students validate AI-generated ESG reports, dashboards, and KPIs, critically examining data reliability, reporting assumptions, and compliance with standards (GRI, TCFD).
  - **Module 5:** Students evaluate AI-based energy predictions, audit results, and optimization strategies, identifying inaccuracies in models, assumptions in energy savings, and practical feasibility.

Research Integration Teaching

Students review on ***at least one recent research topics*** such as:

- Green Data Centers and Sustainable Cloud Computing (energy-efficient computing, cooling systems, carbon reduction strategies)
- Carbon Footprint of AI and Digital Systems (energy consumption of AI models, emissions from data centers)
- Life Cycle Assessment (LCA) in IT Systems (environmental impact from hardware manufacturing to disposal)

- Sustainable Software Engineering and Green AI (energy-aware algorithms, low-power computing)
- ESG and Digital Transformation (role of ESG in technology companies, sustainability reporting and governance)

Students will review at least one recent research paper (journal/conference) in mentioned areas.

NOTE (AI² Pedagogy - Innovative Pedagogy):

1. Each module consists of AI usage, AI evaluation, and human judgment.
    - Students will use AI tools to analyze sustainability problems, such as carbon footprint estimation, ESG scoring, energy consumption prediction, and ethical AI assessment.
    - AI-generated outputs will be critically evaluated using sustainability principles, engineering logic, and real-world benchmarks (e.g., SDGs, ESG metrics, LCA results).
    - Strong emphasis will be placed on validating AI outputs through human judgment, including feasibility, ethical implications, and environmental impact.
    - Students will compare AI predictions with case studies, industry data, or standard frameworks (GRI, TCFD, SDGs) to ensure reliability.

0. Faculty must demonstrate AI use in class, show incorrect AI outputs, and guide students to critique.
    - Demonstration of AI tools for ESG scoring and sustainability analytics, Carbon footprint estimation of IT systems, Energy optimization in data centers and cloud systems, Ethical AI evaluation (bias detection, fairness analysis)
    - Faculty will intentionally present incorrect or biased AI-generated outputs, such as: Misleading ESG scores, Incorrect carbon emission estimates, Biased algorithmic decisions, Unrealistic energy optimization results.
    - Students will be guided to: Identify errors, biases, and incorrect assumptions Analyze limitations of AI models, propose corrected and improved solutions using engineering reasoning and sustainability frameworks.

0. Students must be evaluated on AI-assisted work, AI debugging, and decision-making Assignments will include:
    - AI-generated sustainability analyses (carbon footprint, ESG reports, energy audits) with mandatory validation
    - Case studies involving AI-based sustainability tools and dashboards
    - AI-assisted lifecycle assessment (LCA) and green computing analysis.

0. **Conclusion (Innovative Pedagogy Adopted)**:

    . Teaching AI² Pedagogy:

        . AI-assisted learning using analytical and sustainability tools
        i. Students use AI tools for ESG analysis, carbon footprint estimation, energy prediction, and ethical AI assessment.
        ii. Tools may include AI-driven dashboards, sustainability analytics platforms, and cloud-based simulation environments.

    a. Problem-First Learning (Instead of Topic-First)

        . Start with real-world sustainability challenges such as:

        - "How can data centers reduce their energy consumption and carbon footprint?"
        - "How can cloud computing systems be optimized for sustainability?"

- "How do AI systems impact fairness, privacy, and society?"
- "How can smart cities use IoT for efficient energy management?"

ii. Then introduce concepts and tools like ESG frameworks, carbon accounting, and sustainability metrics, Energy efficiency techniques in computing systems, Lifecycle assessment (LCA) and green computing principles, Ethical AI, bias detection, and governance frameworks.

c. Research-integrated teaching

- Research-oriented course delivery with exposure to modern sustainability applications. Topics include: Green computing and energy-efficient data centers, AI for sustainability and ESG analytics, Smart energy systems and sustainable IoT, Circular economy in digital systems
- Students work on challenges such as: Reducing carbon footprint of IT infrastructure Optimizing cloud resource allocation for energy efficiency, Improving ESG performance using data analytics

d. Sustainability Thinking

i. Energy Impact: Energy efficiency in computing systems, servers, and networks, Energy consumption in data centers and cloud platforms, Optimization of power usage using AI and smart systems

ii. Environmental Impact: Carbon emissions from IT infrastructure, E-waste management and sustainable hardware lifecycle, Environmental implications of large-scale AI models and data processing

iii. Lifecycle Cost and Sustainable Design: Cost-effective and energy-efficient system design, Lifecycle assessment of digital systems

Recommended Tools

- Simulation & Analysis Tools
  Energy modeling and system analysis using MATLAB / Python (NumPy, Pandas, Scikit-learn), Lifecycle Assessment (LCA) tools such as OpenLCA / SimaPro

- Visualization & Dashboard Tools
  Data visualization using Power BI, Tableau, Python (Matplotlib, Seaborn), ESG dashboards and sustainability reporting tools, Smart city and IoT system visualization platforms

- AI & Digital Tools
  AI tools such as ChatGPT for sustainability analysis, report generation, and decision support, Machine learning platforms (TensorFlow, Scikit-learn) for energy prediction and ESG analytics

Suggested Reading

Textbooks

1. Sustainable Computing and the Social Sciences – Lorenz M. Hilty, Bernard Aebischer, 1st Edition, 2015
2. Green IT: Reduce Your Information System's Environmental Impact – Jean-Marc Pierson, 1st Edition, 2012
3. Sustainability Engineering: Concepts, Design and Case Studies – Allen, D. T. & Shonnard, D. R., 1st Edition, 2001.

Reference book

1. Environmental Impact Assessment: Theory and Practice – Glasson, J., Therivel, R., Chadwick, A., 5th Edition, 2012
2. Designing for Sustainability: A Guide to Building Greener Digital Products and Services – Tim Frick, 1st Edition, 2014.

Additional Sources

1. NPTEL – Courses on Sustainable Engineering, Energy Systems, Environmental Studies
2. MIT OpenCourseWare – Courses on Sustainability, Energy, and Smart Systems
3. IEEE, Elsevier, and industry ESG reports for latest research and case studies

AI-Powered Assignments

AI² Pedagogy: *It is a structured teaching-learning approach where students use AI tools for problem-solving while simultaneously developing Authentic Intelligence through critical evaluation, ethical reasoning, and responsible decision-making.*

Assignment 1: AI-Based Energy System Efficiency Evaluation:

- Students use AI tools to analyze energy cycles in sustainability systems such as Data center cooling cycles, HVAC refrigeration systems, Renewable energy-based thermal cycles (e.g., Rankine cycle analogy in energy systems).
- Outputs are validated using energy balance principles, efficiency metrics and real-world benchmark data from sustainability reports. Focus is on energy efficiency and carbon reduction potential.

Assignment 2: AI Debugging in Engineering and Sustainability Systems

- Students are given AI-generated incorrect or biased solutions related to Energy consumption prediction models, ESG scoring or carbon footprint estimation, Flow or thermal system performance analysis.
- Tasks include Identifying logical, numerical, and assumption-based errors, detecting sustainability misinterpretations (e.g., ignoring emissions or losses), Correcting outputs using engineering reasoning and ESG frameworks

Assignment 3: Comparative AI Analysis for Sustainability Decision-Making

- Students compare outputs from multiple AI tools/models for a given sustainability engineering problem such as Energy optimization in cloud/data centers, Carbon footprint estimation of digital systems, Efficiency of cooling or flow-based infrastructure systems.
- Evaluation criteria include: Accuracy and consistency of AI outputs, Assumptions and model limitations, Reliability for real-world engineering decision-making, Environmental and ESG implications

Mini Project Component

- **Industry-Driven Projects**

The following projects simulate real-world engineering and sustainability challenges in digital, energy, and infrastructure systems, integrating AI-based analysis, validation, and decision-making.

Project 1 – Smart Data Center Energy Optimization System

- **Problem:** Design and analyse an energy-efficient data center system to minimize power consumption and carbon footprint.
- **Concepts Used:** Energy efficiency metrics (PUE, energy intensity), Carbon footprint estimation, Resource allocation and load balancing, green computing principles
- **Industry Relevance:** Cloud computing companies, IT infrastructure and data center management, Large-scale enterprise systems

Project 2 – Smart Energy Management System for Buildings/IoT

- **Problem:** Design and simulate a smart system to monitor and optimize energy usage in buildings using IoT and AI.
- **Concepts Used:** Energy audit and consumption analysis, IoT-based monitoring systems, Predictive analytics for energy optimization, Smart grid and automation concepts
- **Industry Relevance:** Smart cities and infrastructure, Building energy management systems, IoT and automation industries

Project 3 – Sustainable Cloud Computing Optimization

- **Problem:** Develop strategies to optimize cloud resource usage for reduced energy consumption and improved sustainability.
- **Concepts Used:** Virtualization and cloud resource allocation, Energy-efficient scheduling algorithms, green cloud computing principles, Lifecycle assessment of cloud services
- **Industry Relevance:** Cloud service providers (AWS, Azure, Google Cloud), IT service companies, SaaS and platform engineering

****

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

DISCRETE MATHEMATICS

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - III

Course Code	**:**	26XXXXX	**Credits**	**:**	02
Hours / Week	**:**	02	**Total Hours**	**:**	30
L–T–P–J	**:**	2–0–0–0		**:**	

Course Vision:

To build a robust theoretical foundation in mathematical logic, counting, and structure that directly enables the analysis, design, and validation of secure computer systems.

Course Objectives:

This Course will enable students to:

1. Learn the set theoretic concept and its application in theory of computation.
2. Determine the concepts of mathematical induction, recursive relations and their application.
3. Illustrate the association of functions, relations, partial ordered set and lattices with problems related to theoretical computer science and network models.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method:** along with traditional lecture method, different type of teaching methods may be adopted to attain the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and roleplaying.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.

6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I	**10 Hours**

SET THEORY: Sets and subsets, Operations on Sets: Basic set operations, algebraic properties of sets, The Addition Principle , **RELATIONS AND ITS PROPERTIES:** Relations and their properties, N-Ary Relations and their applications, Representing relations.

Textbook – 2: 1.1, 1.2; Textbook – 1: 7.1., 7.2, 7.3

Applications: Access Control Systems, Network Security (Firewall Rules), Malware Signature Detection, Vulnerability Management

AI Integration: Feature Engineering in ML, Clustering Attacks, Anomaly Detection

Authentic Intelligence: Efficient threat classification using minimal data, Logical reasoning for zero-trust architectures, Identifying overlaps between attack vectors

NVIDIA DLI Courses (Relevant to this Module):

1. **Accelerating End-to-End Data Science Workflows** (8 hrs) | Path: Data Science Training - Accelerated Data Science Foundations https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-01+V2

MODULE – II	**10 Hours**

RELATIONS AND ORDER RELATIONS: Closure of relations, Equivalence Relations, Partial Orderings, Functions, The Growth of Functions, Transitive Closure and Warshall's Algorithm.

Textbook – 1: 7.4., 7.5, 7.6, 3.2

Applications: Attack Path Discovery, Network Security Analysis, Trust Propagation

AI Integration: Graph traversal algorithms, Threat propagation modeling, Link prediction in security graphs.

Authentic Intelligence: Detecting multi-stage attacks, Understanding lateral movement in networks

MODULE – III	**10 Hours**

MATHEMATICAL INDUCTION AND RECURSION: Mathematical Induction, Recurrence Relations: Rabbits and the Fibonacci Numbers, The Tower of Hanoi, Code word Enumeration, Solving Linear Recurrence Relations, Basic Connectives and Truth Tables

Textbook-1: 4.1;6.1, 6.2;1.1

Applications: Algorithm correctness & analysis, Growth modeling, Forecasting

AI Integration: Formal verification, RNNs, sequences, NLP encoding, Rule-based AI

• **Authentic Intelligence:** Clear decision-making, Eliminating ambiguity in reasoning, Developing structured problem-solving strategies
NVIDIA DLI Free Courses (Relevant to this Module): **1. Accelerating End-to-End Data Science Workflows** (8 hrs) | Path: Data Science Training - Accelerated Data Science Foundations https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-01+V2

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	**Apply** the concepts of set theory, set operations, and relations to model, analyze, and solve practical problems in engineering and computational domains.	L3
2	**Make use of** properties of relations, partial orderings, functions, and growth of functions, along with algorithms like Warshall's Algorithm to analyze, and solve real-world and computational problems.	L3
3	**Utilize** mathematical induction, recursion techniques, linear recurrence relations, and logical connectives to model, analyze, and solve problems in engineering and computing contexts.	L3

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs													
COs	**Program Outcomes (POs)**											**PSOs**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**1**	**2**
CO1	**3**	**2**	**1**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**2**	**1**
CO2	**3**	**1**	**1**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**2**	**1**
CO3	**3**	**2**	**1**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**2**	**1**

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Kenneth H. Rosen, "Discrete Mathematics and its applications", Tata McGraw Hill, 2003.
2. Bernard Kolman, Robert C. Busby, Sharon Ross, "Discrete Mathematical Structures", 3rd Edition, PHI 2001.

REFERENCE BOOKS:

1. Ralph P. Grimaldi, "Discrete and Combinatorial Mathematics", IV Edition, Pearson Education, Asia, 2002.
2. J. P. Tremblay, R. Manohar, "Discrete Mathematical Structures with applications to computer Science", Tata McGraw Hill, 1987.
3. J K Sharma, "Discrete Mathematics", 3rd edition, 2013, Macmillan India Ltd.

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

DIFFERENTIAL EQUATIONS & OPTIMIZATION **[As per Choice Based Credit System (CBCS) scheme]** **SEMESTER - IV**					
Course Code	**: 26AM23XX**		**Credits**	**: 03**	
Hours / Week	**: 03**		**Total Hours**	**: 45**	
L–T–P–J	**: 3–0–0–0**		**CIE+SEE**	**: 60+40 Marks**	
Course Vision: **To develop strong mathematical and computational foundations in differential equations, numerical methods and optimization techniques for solving complex engineering problems and designing intelligent AI-driven optimization systems.**					

Course Objectives:

This course will enable students to:

1. **Apply Laplace transforms and analytical methods to solve differential equations arising in engineering applications.**
2. **Apply numerical methods for solving ordinary and partial differential equations arising in dynamic systems.**
3. **Analyze and solve classical optimization problems encountered in engineering applications.**
4. **Develop problem-solving skills for AI and computational systems.**
5. **Apply nonlinear optimization algorithms to solve complex real-world optimization problems.**

Teaching-Learning Process (General Instructions)

Following are sample new pedagogical methods, where teachers can use to accelerate the attainment of the various course outcomes:

1. **Lecture Method: Concepts, algorithms, and models are explained through structured lectures supported by Python/MATLAB demonstrations.**
2. **Interactive Teaching: Active learning is promoted through discussions, brainstorming, and group problem-solving activities.**
3. **Demonstration using Python/MATLAB: AI techniques like classification and optimization are demonstrated to visualize results and understand implementation.**
4. **Multimedia Learning: Videos and simulations are used to explain complex concepts and real-world applications.**
5. **Collaborative Learning: Students work in groups to implement projects and analyze datasets using computational tools.**
6. **Higher Order Thinking Questions: Analytical questions are used to develop model design,**

evaluation, and decision-making skills.

7. **Problem-Based Learning: Real-world problems are given to apply techniques using Python/MATLAB for practical solutions.**

MODULE – I	09 Hours
Differential Equations **Topics: Introduction to first-order ordinary differential equations (ODE), linear higher order differential equations with constant coefficients, homogeneous and non-homogeneous equations, Existence and uniqueness of solutions for ordinary differential equations, Method of variation of parameters, Introduction of Laplace transforms and its properties, Solving ODE using Laplace transform.** **Applications: Control systems engineering, Electrical circuit analysis, Mechanical vibration systems, Population dynamics modelling**	
MODULE – II	**09 Hours**
Numerical Methods for ODE and PDE **Topics: Solving initial value problems using Taylor series method, Euler's method and modified Euler method, Runge-Kutta methods, multistep methods. Higher-order equations and systems. Stability analysis. Solving boundary value problems using shooting methods, difference methods and variational methods. Introduction to numerical solutions for partial differential equations.** **Applications: Weather prediction models, Mechanical system simulations, Control system modelling, Heat transfer and diffusion problems.**	
MODULE – III	**09 Hours**
Linear Programming **Topics: Linear Programming: Linear programming, standard form of linear programming, geometry of linear programming problems, solution of a system of linear simultaneous equations, pivotal production of general systems of equations, graphical method, simplex algorithms, revised simplex methods, duality in linear programming. Introduction to assignment and transportation problem.** **Applications: Resource allocation and production planning, Transportation and logistics optimization, Supply chain management, Financial portfolio optimization, Scheduling and assignment problems**	

MODULE – IV	09 Hours
Introduction to Optimization **Topics: Introduction to classical optimization, engineering applications of optimization, classification of optimization problems, single variable optimization, multivariable optimization without constraints, multivariable optimization with equality and inequality constraints, Kuhn-Tucker conditions.** **Applications: Resource allocation problems, Engineering design optimization, Production planning, Logistics and supply chain optimization**	
MODULE – V	**09 Hours**
Nonlinear Optimization **Topics: Unconstrained nonlinear optimization, univariate method, gradient of a function, gradient descent method, Fletcher-Reeves method, constrained nonlinear optimization, characteristics of a constrained optimization problem, cutting plane method, interior and exterior penalty function methods.** **Applications: Neural network training, Portfolio optimization, Control system optimization,** **Engineering system design**	

Authentic Intelligence:

1. **Understanding limitations of dynamic models**
2. **Evaluating numerical errors in computational models**
3. **Ethical considerations in automated optimization systems**
4. **Ethical decision-making in optimization problems**
5. **Understanding biases introduced by optimization algorithms**

AI Integration:

1. **Dynamic system modelling in AI robotics**
2. **Simulation of dynamic systems in robotics**
3. **Decision optimization in intelligent systems**
4. **Linear programming used in decision-making systems**
5. **Gradient descent optimization algorithms for training neural networks and deep learning**

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	**Solve ordinary differential equations and apply Laplace transforms for modelling dynamic systems used in AI, signal processing, and control systems.**	**L3**
2	**Implement numerical methods for solving ordinary and partial differential equations arising in engineering and scientific models.**	**L3**

3	**Develop and solve linear programming models for real-world problems**	**L3**
4	**Formulate and solve classical optimization problems including single and multivariable optimization with constraints.**	**L4**
5	**Apply nonlinear optimization techniques such as gradient descent, Fletcher–Reeves method, and penalty methods to engineering applications.**	**L5**

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

	Program Outcomes (POs)											PSOs	
COS	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**1**	**2**
CO-1	3	2			2					1			
CO-2	3	3	2	2	3					1			
CO-3	3	3	3	2	3				1	2			
CO-4	3	3	3	2	2					1			
CO-5	3	3	2	2	3	1		1		1	2		

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. **Erwin Kreyszig, Advanced Engineering Mathematics, 9th Edition, John Wiley & Sons, 2006.**
2. **Boyce W. E. and DiPrima R. C., Elementary Differential Equations and Boundary Value Problems, 9th Edition, Wiley India, 2009.**
3. **Grewal B.S., Higher Engineering Mathematics, Khanna Publishers, 35th Edition, 2010.**
4. **Taha, Hamdy A. *"Operations Research: An Introduction"*, 10th, Pearson Education, 2017.**
5. **Rao, Singiresu S. *Engineering optimization: theory and practice*. John Wiley & Sons, 2019.**

REFERENCE BOOKS:

1. **Bird, John. Higher Engineering Mathematics. 6th ed., Elsevier, 2017.**
2. **Nayak, Sukanta. *Fundamentals of optimization techniques with algorithms*. Academic Press, 2020.**
3. **Arora, R. K. Optimization: Algorithms and Applications. 1st ed., Chapman and Hall/CRC, 2015.**
4. **Deb, Kalyanmoy. Optimization for Engineering Design: Algorithms and Examples. 2nd ed., PHI Learning Pvt. Ltd., 2012.**
5. **Nocedal, Jorge, and Stephen J. Wright. *Numerical Optimization*. 2nd ed., Springer, 2006.**

E-RESOURCES:

RECOMMENDED TOOLS

- **Python**
- **MATLAB**

LAB EXERCISES

S. No	Exercise Title	Aim / Objective	Tools	Hrs	CO
MODULE I: Exercises 1–3: Differential Equations and Transform Methods (03 Hours)					
1	Differential Equations (Basic)	Solve first-order and higher-order differential equations computationally	MATLAB/PYTHON	1 h	CO1
2	Laplace Transform	Use Laplace transforms to solve initial value problems.	MATLAB/PYTHON	1 h	CO1
3	Case Study of Dynamic Modelling	Simulate time-series data using differential equation models.	MATLAB/PYTHON	1 h	CO1
MODULE II: Exercises 4–6: Numerical Methods for ODE & PDE (03 Hours)					

S. No	Exercise Title	Aim / Objective	Tools	Hrs	CO
4	Taylor Series and	Solve ODE using Taylor series method, Euler method and modified Euler method	MATLAB/PYTHON	1 h	

	Euler Method				**CO2**
5	**Runge-Kutta and Multistep Method**	**Implement fourth-order Runge-Kutta method and multistep method**	**MATLAB/PYTHON**	**1 h**	**CO2**
6	**Shooting and Finite Difference Method**	**Solve boundary value problems using shooting and finite difference method**	**MATLAB/PYTHON**	**1 h**	**CO2**
MODULE III: Exercises 7–9: Introduction to Optimization (03 Hours)					
7	**Single Variable Optimization**	**Implement optimization for single variable functions**	**MATLAB/PYTHON**	**1 h**	**CO3**
8	**Multivariable optimization**	**Perform multivariable optimization and their visualization**	**MATLAB/PYTHON**	**1 h**	**CO3**
9	**Kuhn-Tucker Conditions**	**Implement KKT conditions for constrained optimization**	**MATLAB/PYTHON**	**1 h**	**CO3**
MODULE IV: Exercises 10–12: Linear Programming (03 Hours)					
10	**Formulation of LPP**	**Formulate and solve linear programming problems (LPP) and**	**MATLAB/PYTHON**	**1 h**	

		implement graphical method			CO4
11	Simplex Method, Revised Simplex Method	Implement simplex algorithm for LPP, Solve LPP using revised simplex method	MATLAB/PYTHON	1h	CO4
12	Duality in LPP	Analyze duality concepts in	MATLAB/PYTHON	1h	CO4

S.No	Exercise Title	Aim / Objective	Tools	Hrs	CO
		linear programming			
MODULE V: Exercises 13–15: Nonlinear Optimization (03 Hours)					
13	Fletcher-Reeves Method	Implement Fletcher-Reeves optimization method	MATLAB/PYTHON	1h	CO5
14	Cutting Plane Method	Apply cutting plane method for constrained optimization	MATLAB/PYTHON	1h	CO5

15	**Interior and Exterior Penalty Method**	**Implement interior and Exterior penalty function method**	**MATLAB/PYTHON**	**1 h**	**CO 5**

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

CLOUD SECURITY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – IV

Subject Code :		**Credits** :	3
Hours / Week	:03 Hours	**Total Hours** :	45Hours
L–T–P–S :	3–0––0		

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

Course Learning Objectives:

This course will enable students to:

1. Master cloud basics, architecture, and deployment models to improve how your organization manages its IT infrastructure and operations.
2. Master the essential principles and practices of securing cloud-based systems to safeguard data confidentiality, integrity, and availability.
3. Understand and address security risks in cloud computing environments.
4. Understand how to effectively secure cloud computing environments through principles of architecture, trusted methodologies, identity management, and access control.
5. Demonstrate cloud computing life cycle issues, standards, and security measures, and to develop incident response plans.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	08 Hours

Introduction & Cloud Computing Architecture: Cloud computing at a glance: Defining a cloud, A closer look, The cloud computing reference model, Characteristics and benefits Historical developments: Distributed systems, Virtualization, Web 2.0, Service oriented computing, Utility-oriented computing Building cloud computing environments: Application development, Infrastructure and system development, Computing platforms and technologies. The cloud reference model: Architecture, Infrastructure-and hardware-as-a securityservice, Platform as a service, Software as a service .Types of clouds: Public, Private, Hybrid, Open Challenges: Cloud definition, Cloud interoperability and standards, Scalability and fault tolerance, Security, trust, and privacy, Organizational aspects.

UNIT – II	**08 Hours**

Virtualization: Introduction, Characteristics of Virtualized Environments, Taxonomy of Virtualization Techniques - Execution Virtualization, Other types of Virtualization, Virtualization and Cloud Computing, Pros and Cons of Virtualization, Technology Examples – Xen, VMware, Microsoft Hyper-V
Cloud Computing Software Security Fundamentals: Cloud Information Security Objectives- Confidentiality, Integrity, and Availability, Confidentiality, Integrity, Availability, Cloud Security Services- Authentication, Authorization, Auditing, Accountability

UNIT – III	**08 Hours**

Secure Cloud Software Requirement-Secure Development Practices, Approaches to Cloud Software Requirements Engineering, Cloud Security Policy Implementation, NIST 33 Security Principles, *Secure Cloud Software Testing***-**Testing for Security Quality Assurance, Cloud Penetration Testing, Regression Testing.
Cloud Computing Risk Issues and Security Challenges: The CIA Triad, Privacy and Compliance Risks, Threats to Infrastructure, Data, and Access Control, Cloud Service Provider Risks, Cloud Computing Security Challenges**-**Security Policy Implementation, Computer Security Incident Response Team (CSIRT).

UNIT – IV	**08 Hours**

Cloud Computing Security Architecture:
Introduction, ***Architectural Considerations***- General Issues, Trusted Cloud Computing, Secure Execution Environments and Communications, Microarchitectures, ***Identity Management and Access Control***- Identity Management, Access Control, Autonomic Security

UNIT – V	**07 Hours**

Cloud Computing Life Cycle Issues:
Standards, The Distributed Management Task Force (DMTF), The International Organization for Standardization (ISO), The European Telecommunications Standards, The Organization for the Advancement of Structured, Storage Networking Industry Association (SNIA), Open Grid Forum (OGF), The Open Web Application Security Project (OWASP), Incident Response.

Course Outcomes:

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

1. **Analyze** cloud computing fundamentals and architecture to optimize resource utilization and enhance organizational efficiency.
2. **Implement** cloud security measures effectively, including authentication, authorization, and auditing, to ensure confidentiality, integrity, and availability of data in cloud computing environments.
3. **Identify** cloud computing risks and security challenges, applying the CIA triad and privacy regulations. **Evaluate** threats to infrastructure, data, and access control, cloud service providers.
4. **Evaluate** cloud security principles, design secure environments and communications, integrate robust identity management, and enforce access controls for autonomic security.
5. **Assess** and **Analyze** cloud computing life cycle issues, standards from DMTF, ISO, ETSI, SNIA, OGF, and OWASP, and develop incident response plans.

Table: Mapping Levels of COs to POs / PSOs													
COs	**Program Outcomes (POs)**											**PSOs**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**1**	**2**
CO1	3	2	2	1	2	1						2	3
CO2	3	2	3	2	2	1			2			3	3
CO3	2	3	2	3	1	2			3			1	2
CO4	2	3	3	2	2	1			2			2	2
CO5	2	3	2	3	2	1			2	2	1	2	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Rajkumar Buyya, Christian Vecchiola, S Tamarai Selvi "Mastering Cloud Computing Foundations And Applications Programming" , McGraw Hill Education, 2016.
2. Ronald L. Krutz, Russell Dean Vines “Cloud Security A Comprehensive Guide to Secure Cloud Computing” Wiley Publishing. INC.
3. Kai Hwang, Geoffrey C Fox, Jack J Dongarra, "Distributed and Cloud Computing - From Parallel Processing to the Internet of Things", Morgan Kaufman Publishing, 2012

.

REFERENCE BOOKS:

1.Sirisha Potluri et.al. “Cloud Security Techniques and Applications (Smart Computing Applications)”.
2.Chris Dotson, “Practical Cloud Security A Guide for Secure Design and Deployment”. O’Riley Publishing.

E-Resources:

1. National Institute of Standards and Technology (NIST) - Cloud Computing Security: https://www.nist.gov/topics/cloud-computing-security
2. OWASP Cloud Security Top 10: https://owasp.org/www-project-cloud-security-top-10/
3. SANS Institute - Cloud Security: https://www.sans.org/white-papers/cloud-security/
4. Coursera - "Cloud Security Basics" by Google Cloud: https://www.coursera.org/learn/cloud-security-basics
5. edX - "Cloud Computing Security" by University of Maryland: https://www.edx.org/professional-certificate/cloud-computing-security
6. Pluralsight - "Cloud Security" learning path: https://www.pluralsight.com/paths/cloud-security
7. Cybrary - "Cloud Security Fundamentals" course: https://www.cybrary.it/course/cloud-security-fundamentals/

Activity Based Learning (Suggested Activities in Class)

1. Cloud Security as a group Case study.
2. Collaborative Activity is minor project development with a team of 4 students.

LABORATORY EXPERIMENTS

Total Contact Hours: 30

1. Install Oracle Virtual box and create two VMs on your laptop/Desktop.
2. Test ping command to test the communication between the guest OS and Host OS
3. Use gcc to compile c-programs. Split the programs to different modules and create an application using make command
4. Find a procedure to transfer the files from one virtual machine to another virtual machine.
5. Establish an AWS account. Use the AWS Management Console to launch an EC2 instance and connect to it.
6. Launch an EC2 instance in AWS, install and configure CloudWatch and CloudTrail. Simulate an access event and perform basic log analysis to detect the activity.
7. Create a policy in AWS IAM that grants users access to only specific S3 buckets and restricts all other services.
8. Create a new IAM user named john_doe with programmatic access and console access. Attach the following policies to the user: a) AmazonS3ReadOnlyAccess (Read-only access to S3 buckets) b) AmazonEC2FullAccess (Full access to EC2 instances)
9. Implement network-level security in AWS by configuring Security Groups and Network ACLs, restricting inbound and outbound traffic, and validating access through controlled connection attempts.
10. Configure IAM security settings by enabling Multi-Factor Authentication (MFA) for an IAM user named `secure_user` and enforce an account password policy with minimum length, complexity requirements, and password rotation.
11. Use version control systems command to clone, commit, push, fetch, pull, checkout, reset, and delete repositories
12. Demonstrate at least two methods to block access to ChatGPT (or similar AI services) on a system. Implement and verify the blocking using tools like the hosts file, firewall rules, DNS filtering, or proxy settings.

****

EMBEDDED SYSTEM DESIGN

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - IV

Course Code	:		**Credits**	:	04
Hours / Week	:	05	**Total Hours**	:	45+30
L–T–P–J	:	3–0–2–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

To develop the ability to design, analyze, and implement embedded systems by integrating hardware, software, and real-time concepts for solving engineering problems.

Course Objectives:

This course will enable students:

1. To understand the fundamentals and design methodology of embedded systems.
2. To learn ARM architecture and embedded programming concepts.
3. To interface sensors, actuators, and communication protocols.
4. To apply real-time operating systems (RTOS) in embedded applications.
5. To develop embedded systems with communication, security, and power management features.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. Use lecture method along with demonstrations for hardware-software integration.
2. Encourage interactive learning through discussions and problem-solving.
3. Demonstrate real-time applications using development boards.
4. Promote group-based mini projects and hands-on learning.
5. Use simulation tools and IDE-based debugging.
6. Encourage students to design and implement practical embedded solutions.

MODULE – I	**09 Hours**

Introduction to Embedded Systems

Topics: Definition and characteristics of embedded systems, comparison with general-purpose systems, applications, classification, design metrics, processor types (GPP, DSP, FPGA, MCU), memory types, embedded system design flow, UML basics.

Applications: Consumer electronics, automotive systems, industrial automation, Connected devices.

AI Integration: Basic understanding of integrating embedded systems with AI-enabled applications. Use of sensor data for simple intelligent decision-making and introduction to edge and cloud-based processing.

Authentic Intelligence: Understanding constraints of embedded systems in implementing AI and awareness of reliability and real-world deployment challenges.

MODULE – II	**09 Hours**

ARM Architecture & Embedded Programming

Topics: ARM Cortex-M architecture, registers, memory map, pipeline, interrupts, instruction set basics, assembly programming, embedded C programming, compiler optimization, development tools.

Applications: Microcontroller-based control systems, firmware development.

AI Integration: Use of embedded programming to process data for intelligent applications and introduction to AI-enabled firmware design.

Authentic Intelligence: Awareness of efficiency, optimization, and limitations in implementing intelligent algorithms on microcontrollers.

MODULE – III	**09 Hours**

Embedded Hardware & Interfacing

Topics: GPIO, timers, PWM, ADC, DAC, UART, SPI, I2C, CAN basics, sensor interfacing, actuator interfacing, watchdog timer, RTC.

Applications: Sensor-based monitoring systems, motor control systems.

AI Integration: Use of sensor data acquisition and interfacing techniques for AI-based monitoring and control systems.

Authentic Intelligence: Understanding challenges in real-time data accuracy and reliability for intelligent embedded applications.

MODULE – IV	**09 Hours**

Real-Time Operating Systems (RTOS)

Topics: OS basics, real-time systems, tasks, scheduling (RMS, EDF), synchronization (semaphores, mutex), inter-task communication, RTOS basics, RTOS selection.

Applications: Real-time control systems, multitasking embedded devices.

AI Integration: Introduction to real-time task management for intelligent systems and handling multiple processes in AI-based applications.

Authentic Intelligence: Understanding timing constraints and reliability issues in real-time intelligent embedded systems.

MODULE – V	**09 Hours**

Communication Protocols & Embedded Security

Topics: Wired and wireless communication (Wi-Fi, BLE, ZigBee, LoRa), communication protocols (MQTT, HTTP, CoAP), cloud platforms, embedded security basics (encryption, authentication, secure boot), power management.

Applications: Smart home systems, industrial automation, remote monitoring.

AI Integration: Application of communication protocols and embedded systems for data-driven intelligent applications and remote monitoring using connected devices.

Authentic Intelligence: Understanding challenges in secure communication, data reliability, and constraints in implementing intelligent features in embedded systems.

Course Outcomes

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Describe the fundamentals, characteristics, and design methodology of embedded systems.	L2
2	Analyze ARM architecture and develop embedded programs using C/assembly language.	L3
3	Apply interfacing techniques for sensors, actuators, and communication protocols in embedded systems.	L3
4	Apply RTOS concepts such as task scheduling, synchronization, and inter-task communication in embedded applications	L3
5	Develop embedded systems with communication, security, and power management features Techniques for improving the model performance.	L5

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	3	2	2	1	-	-	-	-	-	-	1	2	1
CO2	3	3	2	2	3	-	-	-	-	-	1	3	1
CO3	3	3	3	2	3	-	-	-	2	1	1	2	1
CO4	2	3	3	2	3	2	1	2	2	1	1	2	1

CO5	2	2	3	2	3	2	1	2	2	1	1	2	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Joseph Yiu, The Definitive Guide to ARM Cortex-M3 and Cortex-M4 Processors, 3rd Edition, Elsevier, 2013.
2. Raj Kamal, Embedded Systems: Architecture, Programming and Design, 3rd Edition, Tata McGraw-Hill, 2021.
3. Frank Vahid and Tony Givargis, Embedded System Design: A Unified Hardware/Software Introduction, Wiley, 2002.

REFERENCE BOOKS:

1. E. A. Lee and S. A. Seshia, "Introduction to Embedded Systems: A Cyber-Physical Systems Approach", 2nd Edition, MIT Press, 2017.
2. Patrick Schaumont, "A Practical Introduction to Hardware/Software Co-design", Springer, 2010.
3. Tammy Noergaard, Embedded Systems Architecture: A Comprehensive Guide for Engineers and Programmers, 2nd Edition, Elsevier, 2012.

RECOMMENDED TOOLS

- Programming: Embedded C, C++
- Development Environments (IDE): STM32CubeIDE, Keil uVision, Arduino IDE, Platform
- Hardware Platforms: STM32 (ARM Cortex-M), Arduino (UNO/Nano), ESP32
- Debugging Tools: Serial Monitor, JTAG Debugger (optional)
- Communication Tools: PuTTY, Tera Term
- Networking Tools: MQTT Broker (Mosquitto), ThingSpeak / Blynk
- Simulation Tools (Optional): Proteus, Tinkercad

LAB EXERCISES- 30 Hours

S.No	Exercise Title	Aim / Objective	Tools	Hrs	CO
MODULE I · Exercises 1–3 : Introduction to Embedded Systems (06 Hours)					
1	GPIO Programming	Implement LED blinking and switch interfacing using microcontroller	STM32 (CubeIDE)	2 h	CO1
2	Interrupt Handling	Develop interrupt-based button control for event-driven operation	STM32 (CubeIDE)	2 h	CO1
3	Timer Programming	Generate delay and periodic signals using hardware timers	STM32 (CubeIDE)	2 h	CO1

S.No	Exercise Title	Aim / Objective	Tools	Hrs	CO
MODULE II · Exercises 4–7 : ARM Programming & Interfacing (08 Hours)					
4	PWM Generation	Generate PWM signals to control LED brightness and servo motor	STM32 (CubeIDE)	2 h	CO2
5	ADC Interfacing	Read analog data from sensor and display values	STM32 (CubeIDE)	2 h	CO2
6	UART Communication	Implement serial communication between microcontroller and PC	STM32 (CubeIDE), Tera Term / PuTTY	2 h	CO2
7	SPI Communication	Perform data transfer using SPI protocol with external device	STM32 (CubeIDE)	2 h	CO2
MODULE III · Exercises 8–10 : Embedded Communication & Control (06 Hours)					
8	I2C Communication	Interface I2C-based sensor and read data	STM32 (CubeIDE)	2 h	CO3
9	Motor Control	Control DC motor or servo motor using driver circuit	STM32 (CubeIDE)	2 h	CO3
10	CAN Communication (Demo)	Demonstrate basic CAN communication between nodes	STM32 (CubeIDE)	2 h	CO3
MODULE IV · Exercises 11–12 : RTOS (04 Hours)					
11	RTOS Task Creation	Create multiple tasks and implement scheduling using FreeRTOS	STM32 (CubeIDE with FreeRTOS)	2 h	CO4
12	RTOS Communication	Implement inter-task communication using queue/semaphore	STM32 (CubeIDE with FreeRTOS)	2 h	CO4
MODULE V · Exercises 13–15 : Communication Protocols & Embedded Security (06 Hours)					
13	Wi-Fi Communication	Implement wireless communication and transmit data using Wi-Fi module	ESP32 (Arduino IDE / PlatformIO)	2 h	CO5

S.No	Exercise Title	Aim / Objective	Tools	Hrs	CO
14	Communication Protocol (MQTT/HTTP)	Implement data exchange using MQTT or HTTP protocol	ESP32, MQTT Broker / HTTP Server	2 h	CO5
15	Embedded Security Basics	Demonstrate authentication or basic secure data transmission in embedded system	STM32 / ESP32	2 h	CO5

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - IV

Course Code	:		**Credits**	:	02
Hours / Week	:	02	**Total Hours**	:	30
L–T–P–J	:	1–0–0–2	**CIE+SEE**		

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

Course Vision:

To develop foundational and applied competencies in cybersecurity, enabling learners to understand, analyze, and mitigate cyber threats using modern tools, ethical practices, and intelligent technologies.

Course Objectives: Structural Hazard

The course aims to enable students to:

1. To introduce core principles of cybersecurity and threat landscape
2. To develop skills in securing systems, networks, and applications
3. To provide exposure to cyber laws, risk management, and ethical practices
4. To integrate AI-driven security approaches and authentic intelligence analysis
5. To prepare students for real-world cybersecurity problem-solving

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with traditional lecture method, different types of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I	**09 Hours**

FUNDAMENTALS OF CYBER SECURITY

Topics: Fundamentals of Cyber Security: CIA Triad (Confidentiality, Integrity, Availability), Cyber Security Terminology and Concepts, Types of Cyber Threats: Malware (Virus, Worm, Trojan, Ransomware, Spyware), Phishing and Social Engineering Attacks, Insider Threats and Advanced Persistent Threats (APT), Attack Vectors and Surfaces, Cyber Kill Chain Model.

Applications: Enterprise Security Awareness Programs, Threat Modelling in Organizations, Incident Response Planning

AI Integration: AI-based phishing detection tools, Malware classification using ML models, Threat intelligence platforms (AI-assisted SIEM)

Authentic Intelligence: Human intuition in identifying social engineering, Analyst-driven threat interpretation beyond automated alerts, Ethical decision-making in cyber defense

MODULE – II	**09 Hours**

NETWORK SECURITY **Topics:** Network Security Architecture and Security Concepts, OSI & TCP/IP Security Issues , Common Network Attacks: DoS/DDoS, Man-in-the-Middle (MITM) , Packet Sniffing & Spoofing, Firewalls: Types (Packet Filtering, Stateful, Proxy), Intrusion Detection and Prevention Systems (IDS/IPS), Virtual Private Networks (VPNs), Wireless Network Security (WEP, WPA, WPA3). **Applications:** Secure Network Design, Enterprise Firewall Configuration, Network Traffic Monitoring **AI Integration:** AI-based intrusion detection systems, Network anomaly detection using ML, Automated log analysis tools **Authentic Intelligence:** Human validation of anomaly detection results, Context-aware network defense strategies, Combining intuition with AI alerts	
MODULE – III	**09 Hours**
CRYPTOGRAPHY & DATA SECURITY **Topics:** Introduction to Cryptography, Symmetric Encryption (AES, DES), Asymmetric Encryption (RSA), Hash Functions (SHA family, MD5 limitations), Digital Signatures and Certificates Basics of Public Key Infrastructure (PKI), Key Management and Distribution, Basics of Blockchain Security. **Applications:** Secure Communication Systems, Digital Transactions and E-Commerce, Data Integrity Verification **AI Integration:** AI-assisted cryptanalysis research tools, Blockchain analytics tools, Automated certificate management systems **Authentic Intelligence:** Understanding limitations of encryption, Ethical considerations in cryptographic use, Human oversight in key management	

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		

1	**Understand** the core cybersecurity concepts, security principles (CIA triad), types of cyber threats, and basic cryptographic techniques for protecting information systems.	L3
2	**Apply** network security mechanisms such as firewalls, IDS/IPS, VPNs, and secure protocols to protect data communication and defend against network-based attacks.	L3
3	**Analyze** system and application vulnerabilities, including operating system weaknesses and web application threats (e.g., OWASP Top 10), and recommend appropriate mitigation strategies.	L4

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	3	2	-	-	-	-	-	2	-	-	2	2	1
CO2	3	3	2	2	3	-	-	-	1	-	2	3	3
CO3	3	2	2	-	2	-	-	-	-	-	2	3	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Cybersecurity Essentials, Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short, 1st Edition, Cisco Press (Pearson Education), 2018, ISBN: 978-1587134388
2. Introduction to Cyber Security, The Open University, OpenLearn / The Open University.

REFERENCE BOOKS:

1. William Stallings, Lawrie Brown, Computer Security: Principles and Practice, 4th Edition, Pearson, 2018, ISBN: 978-0134794105.
2. William Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson, 2017, ISBN: 978-0134444284.
3. Dafydd Stuttard, Marcus Pinto, The Web Application Hacker's Handbook, 2nd Edition, Wiley, 2011, ISBN: 978-1118026472.
4. Jon Erickson, Hacking: The Art of Exploitation, 2nd Edition, No Starch Press, 2008, ISBN: 978-1593271442.

RECOMMENDED TOOLS

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

- Security Tools: Wireshark, Nmap, Metasploit, Burp Suite
- SIEM Tools: Splunk, IBM QRadar
- AI/ML Tools: Python (Scikit-learn, TensorFlow), Weka
- Cloud Security: AWS Security Hub, Azure Defender
- Forensics Tools: Autopsy, FTK

INTRODUCTION TO DATA SCIENCE

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - IV

Course Code	:		**Credits**	:	02
Hours / Week	:	2	**Total Hours**	:	30
L–T–P–J	:	2–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

To provide foundational knowledge of data science concepts, statistical analysis, data preprocessing, and visualization techniques for solving real-world problems across multiple engineering domains.

Course Objectives:

This course will enable students:

1. Understand fundamental data science concepts and workflows
2. Apply statistical techniques and visualization for data analysis
3. Perform data cleaning and preprocessing
4. Use feature selection and dimensionality reduction methods
5. Gain exposure to scalable data analytics techniques

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with traditional lecture method, different types of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I	**06 Hours**

Basic Concepts and Python Packages

Topics: Predictive Modelling, Introduction: Data Preparation, Importance of Data Preparation, Data Cleaning, Feature Selection, Data Transformation, Python Packages: NumPy, Matplotlib, Pandas, SciPy, Scikit-learn, DataFrames, Loading Machine Learning Data

Applications: Data preprocessing in real-world problems, Basic analytics workflows

AI Integration: Data preparation for AI systems

Authentic Intelligence: Understanding data quality and reliability

MODULE – II	**06 Hours**

Descriptive Statistics and Data Visualization

Topics: Sampling, Data Analysis Process, Mean, Median, Standard Deviation, Skewness, Kurtosis, Data Visualization Techniques: Box Plot, Scatter Plot, Histogram, Bar Chart, Pie Chart, Heat Map, Correlation Analysis, Pivot Tables, ANOVA, Data Preprocessing, Rescaling, Standardization, Normalization, Binarization, Univariate and Bivariate Analysis, Recursive Feature Elimination, Principal Component Analysis

Applications: Data analysis and reporting, Visualization-driven decision making

AI Integration: Statistical modeling and visualization in AI

Authentic Intelligence: Interpreting statistical and visual insights correctly

MODULE – III	**06 Hours**

Server-Side Development with Node.js and Express.js

Topics: Handling Missing Data, Outlier Detection and Removal, Statistical Imputation, KNN Imputation, Iterative Imputation, Feature Selection Techniques, Methods for Categorical and Numerical Data, Feature Selection for Outputs, Recursive Feature Elimination, Importance of Feature Selection

Applications: Data cleaning in industry datasets, Feature engineering workflows

AI Integration: Improving model performance through feature selection

Authentic Intelligence: Ensuring reliable and unbiased data

MODULE – IV	**06 Hours**

Databases for Web Applications

Topics: Data Transformation and Dimensionality Reduction: Scaling Techniques, Min-Max Scaling, Standard Scaling, Handling Outliers, Encoding Categorical Data, Transforming Data Distributions, Feature Engineering, PCA, LDA, SVD Techniques

Applications: Data transformation pipelines, High-dimensional data analysis

AI Integration: Feature optimization for machine learning

Authentic Intelligence: Reducing complexity while preserving information

MODULE – V	**06 Hours**

Web Security, Performance, and Deployment

Topics: CPU vs GPU in Data Processing, Need for Fast Data Analytics, Introduction to RAPIDS, GPU-Accelerated Data Workflows, Handling Large Datasets Efficiently, Basic Concept of Accelerated DataFrame Operations, Overview of Machine Learning Acceleration, Identifying Processing Bottlenecks, Real-World Applications of Accelerated Data Analytics, Case study-population-scale data analysis for epidemic control, Integration of multiple datasets, Real-time data analysis and iterative model updates, Decision-making using large-scale data insights

Applications: Large-scale data analysis, Real-time decision-making systems

AI Integration: GPU-accelerated ML pipelines, High-performance AI systems

Authentic Intelligence: Efficient handling of large datasets, Scalable and reliable data-driven solutions

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Explain basic data science concepts and data preprocessing techniques	L2
2	Apply statistical methods and visualization techniques for data analysis	L3
3	Perform data cleaning and feature selection for efficient data preparation	L4
4	Apply data transformation and dimensionality reduction techniques	L3
5	Understand scalable data analytics concepts using modern tools	L2

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2

CO1	**2**	**2**	**3**	**-**	**2**	**-**	**-**	**-**	**-**	**1**	**-**	**2**	**2**
CO2	**2**	**3**	**3**	**1**	**2**	**-**	**-**	**-**	**1**	**1**	**-**	**2**	**2**
CO3	**3**	**3**	**3**	**2**	**3**	**1**	**-**	**-**	**2**	**1**	**1**	**3**	**2**
CO4	**3**	**3**	**2**	**2**	**3**	**1**	**-**	**-**	**1**	**1**	**1**	**3**	**2**
CO5	**3**	**3**	**2**	**2**	**3**	**2**	**1**	**1**	**2**	**2**	**2**	**3**	**2**

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

REFERENCE BOOKS:

1. Joel Grus – Data Science from Scratch
2. Wes McKinney – Python for Data Analysis
3. Jake VanderPlas – Python Data Science Handbook
4. Online documentation (Pandas, Scikit-learn, Matplotlib)
5. DLILink:https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+T-DS-03+V1#:~:text=The%20course%20prerequisites%20include:%20*%20Basic%20understanding,the%20NVIDIA%20Deep%20Learning%20Institute%20at%20www.nvidia.com/dli

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

AI Essentials for Cyber Security

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – IV

Subject Code	:	Credits	: 04
Hours / Week	: 03 Hours	Total	: 45 (Th)+30(P)Hours
L–T–P–J	: 3–0–2–0		

Course Learning Objectives:

This course will enable students to:

1. Understand the fundamentals of Artificial Intelligence, Machine Learning, and their applications in cyber security.
2. Analyze cyber threats using intelligent data-driven techniques.
3. Apply supervised, unsupervised, and ensemble learning models for cyber security problems.
4. Design AI-enabled solutions for anomaly detection, phishing detection, and network defense.
5. Explore Generative AI, Large Language Models (LLMs), prompt engineering, and AI-assisted threat intelligence.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I Introduction to AI-ML	**09 Hours**

Introduction to Artificial Intelligence and Machine Learning, Evolution of AI in Cyber Security, Cyber threat landscape and intelligent defense systems, Types of Machine Learning Algorithms- Supervised Learning,Unsupervised Learning,Reinforcement Learning; Data preprocessing and feature engineering,ML pipeline architecture- Training, validation, and testing concepts, Overfitting, Underfitting, Bias, Variance, Classification and prediction techniques, Introduction to cyber security datasets, Challenges in AI-driven cyber defense
Applications- Malware classification,Intrusion detection systems,Intelligent firewall systems,AI-assisted threat prioritization,Security log analysis AI Integration- Using Python libraries for ML model creation,Introduction to Scikit-learn and Jupyter Notebook,AI-based cyber analytics dashboards Authentic Intelligence Integration-Responsible AI usage in cyber security,Bias and fairness in security datasets,Human-in-the-loop cyber defense

UNIT – II Time Series Analysis	**12 Hours**
Introduction to Time Series Forecasting, Components of Time Series Data-Trend, Seasonality, Noise, Cyclic behaviour; Time Series decomposition techniques, Cyber security event forecasting, DDoS attack prediction using ML, Classification and Regression Algorithms- Binary and Multi-Class Classification, Regression - Linear Regression and Nonlinear Regression, Logistic Regression, Decision Trees (ID3, CART) and Random Forest, Regularization - L1 Regularization, L2 Regularization Ensemble Learning Methods, Voting and Stacking techniques, Bagging Algorithms, Understanding Out-Of-Bag Score, Boosting: AdaBoost, Gradient Boosting Machines (GBM), XGBoost, CatBoost.	
Applications- DDoS attack forecasting, Network traffic prediction, User behavior analytics, Security event forecasting AI Integration- Ensemble-based cyber attack prediction, AI-driven anomaly trend analysis Authentic Intelligence Integration- Trustworthy forecasting systems, Ethical use of behavioral analytics, Minimizing false positives in intelligent defense systems	

UNIT – III Malicious URL Detection	**09 Hours**

Introduction to malicious URLs and phishing attacks, Types of URL-based cyber attacks, Feature extraction from URLs, Heuristic-based malicious page detection, Machine Learning approaches for URL classification- Logistic Regression for phishing detection, Support Vector Machine (SVM), Browser security analytics, AI-enabled phishing detection systems

Applications- Phishing website detection, Fake domain identification, Browser security extensions

AI Integration- AI-assisted phishing detection platforms, Real-time malicious URL classifiers

Authentic Intelligence Integration- Ethical use of user browsing data, Privacy-preserving web security analytics, Human verification in AI-generated alerts

UNIT – IV CAPTCHA Analysis, and Network Anomaly Detection	**09 Hours**

Fundamentals of CAPTCHA systems, Characteristics and types of CAPTCHA, AI techniques used to crack CAPTCHA, Defensive CAPTCHA mechanisms, Email Spoofing attacks, Spam detection using Machine Learning, Clustering techniques in cyber security- K-Means clustering algorithm; Network anomaly detection using clustering, Insider threat detection basics. Machine Learning Optimization Algorithms: Gradient Descent Techniques, Bayesian Optimization, Overfitting, Underfitting, Optimal Fit, Bias, Variance, Regularization - L1 Regularization, L2 Regularization, Elastic Net Regularization.

Applications- Spam email filtering systems, Email fraud detection, Network anomaly monitoring, Insider threat detection

AI Integration- AI-powered spam filters, Intelligent network monitoring systems

Authentic Intelligence Integration- Ethical AI in email surveillance, Trustworthy anomaly detection systems, Responsible monitoring and privacy preservation

UNIT – V Intelligent Threat Analysis & LLMs	**09 Hours**

Context-based malicious event detection ,Event correlation and behavioral analysis ,Rule-based vs AI-based threat detection systems ,Security incident classification using Decision Trees ,Threat intelligence and attack pattern analysis ,Introduction to Generative AI in cyber security , Fundamentals of Large Language Models (LLMs) ,Transformer architecture basics ,Tokenization and embeddings , Prompt Engineering fundamentals ,Types of prompts:Zero-shot prompting,Few-shot prompting ,Chain-of-thought prompting; AI-powered threat analysis and cyber intelligence, Automated incident response using AI

Applications- Intelligent malware detection system, Automated cyber incident summarization, Context-aware intrusion detection

AI Integration- Using LLMs for threat intelligence generation , Prompt engineering for cyber investigation workflows

Authentic Intelligence Integration- Human-in-the-loop security decision systems , Responsible use of Generative AI in cyber defense

Course Outcomes		
Course Outcomes (COs)	**Description**	**Bloom's Taxonomy Level**
At the end of the course the student will be able to:		
1	Illustrate the fundamental concepts of Artificial Intelligence, Machine Learning, and cyber security analytics	**L2**
2	Apply supervised, unsupervised, and ensemble learning algorithms suitable for cyber security problems	**L3**
3	Identify malicious URLs, phishing attacks, spam emails, and network anomalies using intelligent techniques	**L3**
4	Illustrate predictive threat analysis and cyber defense automation	**L2**
5	Explain LLMs, and Authentic Intelligence principles for trustworthy and ethical cyber security systems.	**L2**

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	3	2	2	2	1				1			1	2	1
CO2	2	1			2				1			2	2	2
CO3	3	3	2	2	3							1	2	2
CO4	3	2		1	2		2	3				2	2	2
CO5	3	2	1	1	3		1	3				2	2	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. A. Hands-on Machine Learning for Cyber Security by Soma Halder, ISBN139781788992282
2. Machine Learning – Tom M. Mitchell, McGraw-Hill, 1st Edition, 1997
3. Hands-On Machine Learning with Scikit-Learn, Keras & TensorFlow – Aurélien Géron, O'Reilly Media, 3rd Edition, 2022.

REFERENCE BOOKS:

1. Pattern Recognition and Machine Learning – Christopher M. Bishop, Springer, 1st Edition, 2006.
2. Introduction to Machine Learning with Python – Andreas C. Müller & Sarah Guido, O'Reilly Media, 1st Edition, 2017.

RECOMMENDED TOOLS

- Programming: Python (NumPy, Pandas, Scikit-learn, PyTorch) – Google Colab/ Jupyter Notebook/Visual Studio
- Visualization: Matplotlib, Seaborn, Plotly, UMAP
- Experiment Tracking: MLflow, Weights & Biases
- MLOps & Deployment: Docker, FastAPI, ONNX
- AI Assistants: GitHub Copilot, ChatGPT, Claude

LAB EXERCISES – 30 Hours

S.No	Exercise Title	Aim / Objective	Tools	Hrs	CO
1	Data Analysis and Visualization	Perform Exploratory Data Analysis and Visualize Features using the suitable Dataset (e.g: Iris Dataset)	Google Colab/ Jupyter	2 h	CO1
2	Handling Missing Values, Scaling Features	Preprocess Data by Handling Missing Values, Encoding Categorical Variables, and Scaling Features on Standard Dataset.	Google Colab/ Jupyter	2 h	CO1
3	Split Dataset, cross validation	Split Dataset into Training and Testing Sets and Apply Cross-Validation.	Google Colab/ Jupyter	2 h	CO1
4	Linear Regression	Implement Linear Regression to Predict House Prices using the Housing Price Dataset.	Google Colab/ Jupyter	2 h	CO2
5	Logistic Regression	Build a Logistic Regression Model to Perform Classification	Google Colab/ Jupyter	2 h	CO2
6	K-Nearest Neighbors (KNN)	Apply the K-Nearest Neighbors (KNN) Algorithm to perform classification on suitable dataset (e.g Classify Flower Species using the Iris Dataset)	Google Colab/ Jupyter	2 h	CO2
7	Decision Tree Model	Train and Visualize a Decision Tree Model to perform Classification (e.g. Wine Quality using the Wine Quality Dataset)	Google Colab/ Jupyter	2 h	CO2
8	Random Forest Model	Develop a Random Forest Model to perform Prediction. (e.g: Heart Disease using the Heart Disease Dataset)	Google Colab/ Jupyter	2 h	CO2
9	K-Means Clustering	Apply K-Means Clustering to Perform Customer Segmentation. (e.g using the Mall Customer Segmentation Dataset)	Google Colab/ Jupyter	2 h	CO3
10	Principal Component Analysis	Apply Principal Component Analysis (PCA) to Reduce Feature Dimensions. (e.g: using the Wine Dataset)	Google Colab/ Jupyter	2 h	CO3
11	**Model evaluation**	Evaluate Classification Models by Computing Accuracy, Precision, Recall, F1-Score, and Confusion Matrix using dataset (e.g Breast Cancer Dataset)	Google Colab/ Jupyter	2 h	CO5

S.No	Exercise Title	Aim / Objective	Tools	Hrs	CO
12	Machine Learning Model to Solve a Real-World Engineering	Design and Implement a Machine Learning Model to Solve a Real-World Cyber Security Problem using an Open Engineering Dataset	Google Colab/ Jupyter	2 h	CO5

WEB TECHNOLOGIES

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - IV

Course Code	:		**Credits**	:	02
Hours / Week	:	2	**Total Hours**	:	30
L–T–P–J	:	2–0–0–0	**CIE**	:	10 Marks

Course Vision:

To equip students with industry-relevant skills in designing, developing, and deploying modern web applications by integrating foundational web standards, client-side and server-side technologies, database connectivity, security practices, and cloud deployment - preparing them to contribute effectively to real-world software engineering projects and entrepreneurial ventures in the digital economy.

Course Objectives:

This course will enable students:

1. Understand the architecture of the World Wide Web, HTTP/HTTPS protocols, and apply HTML5 and CSS3 to build semantically structured, responsive web pages.
2. Develop dynamic, interactive client-side applications using JavaScript, its modern ES6+ features, and the DOM API.
3. Design and implement server-side RESTful web services and back-end logic using Node.js and Express.js.
4. Integrate SQL and NoSQL (MongoDB) databases with web applications for persistent and efficient data management.
5. Apply web security principles, performance optimization techniques, and deploy web applications on cloud platforms responsibly.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with traditional lecture method, different types of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I	**06 Hours**

Web Fundamentals, HTML5 and CSS3

Topics: Web Fundamentals: Client–Server Architecture, Web Browsers, URL and DNS Basics, HTTP & HTTPS: Request–Response Lifecycle, HTTP Methods, Status Codes, HTML5: Document Structure, Semantic Elements, Forms, Multimedia, CSS3: Selectors, Box Model, Flexbox, CSS Grid, Responsive Web Design, Basic Transitions and Animations.

Applications: Static and responsive multi-page web portals, Portfolio and resume websites, Online form interfaces for data collection, Accessible government and educational websites

AI Integration: AI tools (GitHub Copilot, ChatGPT) for accelerated HTML/CSS scaffolding and debugging, Automated accessibility testing using AI-based tools, AI-powered responsive design suggestions (Adobe Firefly, Framer AI), Code linting and best-practice enforcement via AI-integrated IDEs.

Authentic Intelligence: Understanding that AI-generated HTML must be manually validated for semantic correctness and accessibility, Critical evaluation of auto-generated CSS for performance and maintainability

NVIDIA DLI Courses (Relevant to this Module):

1. **Getting Started with Deep Learning** (8 hrs) | Path: Deep Learning — Foundational Deep Learning for AI-Driven Web Applications
   https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+C-FX-01+V3
2. **Building Real-World AI Applications with NVIDIA NIM** (2 hrs) | Path: Generative AI — Deploying LLM Microservices via REST APIs
   https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-NIM-01+V1

MODULE – II	**06 Hours**

JavaScript and Client-Side Development

Topics: JavaScript Fundamentals: Variables, Data Types, Scope, Functions, Conditionals and Loops, ES6 Features: Arrow Functions, Template Literals, Destructuring, Spread Operator, DOM Manipulation, Event Handling, Asynchronous JavaScript: Promises and Async/Await, Fetch API, Client-Side Storage: localStorage, sessionStorage, Cookies.

Applications: Dynamic form validation and real-time feedback, Single-page interaction without page reloads, Browser-based games and interactive dashboards, Client-side data filtering and search

AI Integration: AI-assisted JavaScript debugging (GitHub Copilot, Tabnine), AI-powered code review for detecting runtime errors

Authentic Intelligence: Responsible use of asynchronous patterns to prevent UI blocking and poor UX, Security implications of storing sensitive data in localStorage

MODULE – III	**06 Hours**

Server-Side Development with Node.js and Express.js

Topics: Node.js Fundamentals: Event-Driven Architecture, npm and package.json, Built-in Modules, Express.js: Application Setup, Routing, Request and Response Handling, Middleware, RESTful API Development, Template Engine Basics (EJS), Authentication and Authorization, Password Hashing with bcrypt.

Applications: RESTful back-end APIs for mobile and web frontends, Authentication services for SaaS platforms, File upload and download services

AI Integration: Integrating OpenAI / Anthropic APIs via Node.js HTTP clients, AI-assisted, API documentation generation (Swagger + AI), Intelligent rate limiting and anomaly detection using AI middleware

Authentic Intelligence: Secure storage of credentials - avoiding hardcoded secrets (use .env and dotenv), JWT expiry and refresh token strategies to balance security and UX

NVIDIA DLI Free Courses (Relevant to this Module):

1. **Building Conversational AI Applications** (8 hrs) | Path: Conversational AI — Integrating LLM APIs via Node.js REST Back-Ends

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-FX-17+V1

MODULE – IV	**06 Hours**

Databases for Web Applications

Topics: Relational Databases: SQL Basics, DDL and DML Operations, Keys and JOINs, Preventing SQL Injection, Connecting Databases with Node.js, NoSQL and MongoDB Basics, MongoDB CRUD Operations, Query Operators, Indexing and Aggregation Basics, Mongoose ODM: Schemas, Models, Validation, and Populate.

Applications: User profile and credential management systems, Real-time analytics dashboards backed by MongoDB aggregation, Mechanical vibration systems, Healthcare patient record management systems

AI Integration: AI-assisted query optimization and schema suggestions, Intelligent database indexing recommendations

Authentic Intelligence: Data privacy and GDPR compliance - responsible storage of personal data, Preventing SQL injection through parameterized queries and ORMs

NVIDIA DLI Courses (Relevant to this Module):

1. **Introduction to AI in the Data Center** (1 hrs) | Path: Infrastructure — AI-Ready Database Architecture & Cloud Storage Design

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+T-FX-01+V1

MODULE – V	**06 Hours**

Web Security, Performance, and Deployment

Topics: Web Security: XSS, CSRF, SQL Injection Prevention, HTTPS, CORS, Secure HTTP Headers, Web Performance Optimization: Minification, Lazy Loading, Image Optimization, Caching, Progressive Web Apps (PWA) Basics, WebSockets and Real-Time Communication, Cloud Deployment: Environment Variables, Node.js Application Deployment, CI/CD Basics, Domain and DNS Basics.

Applications: Secure banking and fintech web portals, Real-time collaborative tools (Google Docs-style)

AI Integration: AI-powered vulnerability scanning, AI-assisted performance profiling

Authentic Intelligence: Responsibility for securing user data against web vulnerabilities, Environmental cost of cloud computing - choosing efficient deployment architectures
NVIDIA DLI Free Courses (Relevant to this Module): 1. **AI Security Fundamentals: Protecting Deployed Web AI Systems** (1 hr) | Path: AI Security Engineering — OWASP AI Top-10, DevSecOps & Container Security https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-03+V1

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Explain the fundamentals of web technologies, HTTP/HTTPS, and create structured web pages using HTML5 and CSS3.	L2
2	Develop responsive and interactive front-end web applications using JavaScript, DOM manipulation, event handling, and asynchronous programming.	L3
3	Build server-side web applications and RESTful APIs using Node.js, Express.js, middleware, and authentication mechanisms.	L3
4	Apply SQL and MongoDB database operations for designing and integrating data-driven web applications.	L3
5	Implement basic web security practices, optimize web application performance, and deploy applications to cloud platforms.	L4

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs													
COs	**Program Outcomes (POs)**											**PSOs**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**1**	**2**
CO1	**2**	**2**	**3**	**-**	**2**	**-**	**-**	**-**	**-**	**1**	**-**	**2**	**2**
CO2	**2**	**3**	**3**	**1**	**2**	**-**	**-**	**-**	**1**	**1**	**-**	**2**	**2**
CO3	**3**	**3**	**3**	**2**	**3**	**1**	**-**	**-**	**2**	**1**	**1**	**3**	**2**
CO4	**3**	**3**	**2**	**2**	**3**	**1**	**-**	**-**	**1**	**1**	**1**	**3**	**2**
CO5	**3**	**3**	**2**	**2**	**3**	**2**	**1**	**1**	**2**	**2**	**2**	**3**	**2**

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. HTML & CSS: Design and Build Web Sites by Jon Duckett
2. JavaScript: The Definitive Guide, Seventh Edition by David Flanagan
3. JavaScript and JQuery: Interactive Front-End Web Development by Jon Duckett
4. Web Development with Node and Express, 2nd Edition by Ethan Brown
5. MongoDB: The Definitive Guide, 3rd Edition by Shannon Bradshaw, Eoin Brazil, Kristina Chodorow

REFERENCE BOOKS:

1. Douglas Crockford, JavaScript: The Good Parts, O'Reilly Media, 1st Edition
2. Thomas A. Powell, HTML & CSS: The Complete Reference, McGraw-Hill

RECOMMENDED TOOLS

- Frontend: HTML5, CSS3, JavaScript (ES6+), React.js (optional but recommended),Bootstrap / Tailwind CSS
- Backend: Node.js, Express.js, Postman / Thunder Client
- Databases: MongoDB (Atlas), MySQL / PostgreSQL
- Dev Tools: Visual Studio Code, Git & GitHub
- Deployment: Vercel / Netlify (frontend), Render / AWS (backend)
- AI Assistants: GitHub Copilot, ChatGPT, Claude

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

DevOps

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - IV

Course Code	:		**Credits**	:	02
Hours / Week	:	2	**Total Hours**	:	30
L–T–P–J	:	2–0–0–0	**CIE**	:	100 Marks

Course Vision:

To build industry-ready software engineering professionals who can design, automate, and operate the complete software delivery lifecycle - from source-code management and automated testing through containerisation, orchestration, cloud deployment, and site reliability engineering - by internalising an automation-first, security-by-design, and blameless-culture mindset that accelerates delivery while ensuring system resilience, observability, and responsible stewardship of infrastructure.

Course Objectives:

This course will enable students:

1. To understand the DevOps philosophy, cultural principles (CALMS framework, Three Ways), and the complete software delivery lifecycle from commit to production.
2. To apply Linux system administration, Bash scripting, and advanced Git version-control workflows essential for automating and managing DevOps processes.
3. To design and implement automated CI/CD pipelines using GitHub Actions and Jenkins, integrating code-quality gates, security scanning, artifact management, and Infrastructure as Code with Terraform and Ansible.
4. To containerise applications using Docker and orchestrate production workloads on Kubernetes, configuring services, ingress, auto-scaling, and Helm-based package management.
5. To implement cloud-native DevOps on AWS/GCP/Azure, integrate DevSecOps security practices, configure an observability stack (Prometheus, Grafana, ELK), and apply Site Reliability Engineering principles including SLOs and error budgets.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with traditional lecture method, different types of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I	**06 Hours**

DevOps Foundations, Linux System Administration & Advanced Git

Topics: DevOps Fundamentals (Philosophy, CALMS, Three Ways, DevOps vs Agile vs SRE, DORA Metrics), DevOps Lifecycle & Toolchain (Plan to Monitor, Tool Ecosystem, Value Stream Mapping), Linux Basics for DevOps (Filesystem, Commands, Permissions, Processes, Package Management, SSH & File Transfer), Bash Scripting (Conditionals, Loops, Functions, Error Handling, Scheduling), Networking Basics (OSI/TCP-IP, DNS, HTTP/HTTPS, Ports, Network Tools, Firewall & SSH), Git & Version Control (Git Internals, Branching Strategies, History Management, Collaboration & Code Review, Versioning).

Applications: Automated server initialisation Bash script (EC2 user-data style) — installs packages, creates users, configures SSH, Log-parsing pipeline using grep + awk + sed to extract error rates from Nginx access logs, Scheduled daily backup automation with cron: database dump → gzip → upload to cloud object storage

AI Integration: GitHub Copilot for Bash script generation, documentation, and unit test scaffolding, Natural language to shell command translation using LLMs (Claude CLI, ChatGPT) for DevOps automation, LLM-generated runbooks and post-mortem templates from incident alert context

Authentic Intelligence: Never blindly execute AI-generated scripts - mandatory review for destructive operations (rm -rf, DROP TABLE) and privilege escalation, Ethical responsibility: a poorly tested cron job can cause a production outage affecting thousands of users

NVIDIA DLI Courses (Relevant to this Module):

1. Fundamentals of Linux for DevSecOps and Infrastructure Automation (Free | ~4 hrs) | Path: Infrastructure & DevOps — Foundations

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+T-SY-01+V1

MODULE – II	**06 Hours**

Containerisation with Docker & Container Registry Management

Topics: Containers & Virtualization Basics (Containers vs VMs, Namespaces, cgroups, Union Filesystems, OCI), Docker Architecture (Docker Daemon, CLI, containers, runc, Client–Server Model), Dockerfile & Image Building (Core Instructions, Multi-stage Builds, Layer Caching, Base Images, Security Best Practices), Docker CLI & Runtime (Build, Run, Exec, Logs, Resource Limits, Restart Policies), Docker Networking & Storage (Network Types, DNS, Port

Mapping, Volumes, Bind Mounts, Persistence), Docker Compose (Service Configuration, Dependencies, Environment Management, Multi-environment Setup), Container Registry & Image Management (Docker Hub/GHCR/ECR, Tagging Strategies, Multi-arch Builds, Image Scanning)

Applications: Multi-stage Dockerfile for a Python FastAPI service - builder stage (pip install) + distroless final image, reducing image size by over 80%, Containerising a legacy monolith by extracting it into a reproducible Docker image with environment-based configuration

AI Integration: GitHub Copilot for generating Dockerfiles, .dockerignore, and docker-compose.yml with context-aware multi-stage suggestions, AI-assisted Dockerfile linting and security hardening (Hadolint + Semgrep rules integrated with Git pre-commit hooks)

Authentic Intelligence: Never run containers as root in production — principle of least privilege reduces blast radius of container escapes, SHA digest pinning over mutable tags (latest) prevents silent supply-chain attacks from upstream image tampering

MODULE – III	**06 Hours**

CI/CD Pipelines, Infrastructure as Code & Configuration Management

Topics: CI/CD Fundamentals (CI vs CD, Pipeline Stages, Pipeline as Code, Shift-left Testing), GitHub Actions (Workflows, Triggers, Runners, Reusable Workflows, Secrets, Caching, Matrix Builds, Deployments), Jenkins (Master–Agent, Jenkinsfile, Pipeline Stages, Shared Libraries, Docker Integration), Code Quality & Security (Static Analysis, Pre-commit Hooks, Dependency Scanning, Quality Gates), Artifact Management (Artifacts, Repositories, Versioning & Promotion), Infrastructure as Code with Terraform (HCL, Providers, State Management, Lifecycle, Modules, Workspaces), Configuration Management with Ansible (Inventory, Playbooks, Roles, Variables, Templates, Vault, Idempotency), GitOps Basics (Principles, Pull vs Push CD, ArgoCD Overview)

Applications: Jenkins multi-branch pipeline for a Java Spring Boot service with SonarQube quality gate and Nexus artifact promotion, Ansible playbook for zero-downtime rolling deployment of a web application across 10 VMs with pre/post health checks

AI Integration: AI-generated Terraform modules and Ansible playbooks using GitHub Copilot and Amazon CodeWhisperer, AI-powered IaC security scanning using Checkov and tfsec with LLM-generated remediation explanations

Intelligent rate limiting and anomaly detection using AI middleware

Authentic Intelligence: Immutable infrastructure principle: resist the temptation to SSH into production and patch manually ('pets vs cattle') — every change must flow through a pipeline, Responsible use of CI secrets: masked variables can still leak through log interpolation — audit pipeline logs before making repositories public

NVIDIA DLI Free Courses (Relevant to this Module):

1. Building CI/CD Pipelines for Machine Learning and AI Workloads on GPU Infrastructure (4 hrs) | Path: MLOps & DevOps for AI — Production AI Pipeline Engineering

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-FX-22+V1

MODULE – IV	**06 Hours**

Container Orchestration with Kubernetes & Observability Stack

Topics: Kubernetes Fundamentals (Architecture, Control Plane & Worker Nodes, Networking, CNI, Declarative vs Imperative), Core Kubernetes Objects (Pod, ReplicaSet, Deployment, StatefulSet, DaemonSet, Jobs, Namespaces), Services & Ingress (Service Types, Ingress, DNS & Service Discovery), Configuration & Storage (ConfigMaps, Secrets, Volumes, PV/PVC, StorageClasses), Resource Management & Scaling (Requests/Limits, Quotas, HPA, Autoscaling), Helm (Charts, Templates, Releases, Repositories, Configuration Overrides), Kubernetes Security (RBAC, Service Accounts, Pod Security, Network Policies, Secrets Management), Observability (Monitoring with Prometheus & Grafana, Logging with EFK, Distributed Tracing & OpenTelemetry)

Applications: Deploy a 3-tier microservices application on Kubernetes with Deployments, ClusterIP and LoadBalancer Services, Nginx Ingress with TLS, ConfigMaps for environment config, and HPA targeting 70% CPU, Full kube-prometheus-stack installation: Prometheus scraping custom application metrics, Grafana dashboards with SLO burn-rate panels, Alertmanager Slack integration

AI Integration: k8sGPT for natural-language Kubernetes cluster diagnostics — AI interpretation of CrashLoopBackOff, Pending pods, and resource quota breaches, AI-powered anomaly detection in Prometheus time-series metrics (Amazon DevOps Guru, Dynatrace Davis AI, Grafana ML)

Authentic Intelligence: CPU/memory limits are not optional in production - unbounded containers cause noisy-neighbour eviction of critical services, RBAC misconfiguration is the number-one Kubernetes security finding in cloud audits — least-privilege must be designed from day one, not retrofitted

NVIDIA DLI Courses (Relevant to this Module):

1. **Deploying AI Workloads on Kubernetes with NVIDIA GPU Operator and Multi-Instance GPU (MIG) (8 hrs) | Path: Infrastructure & DevOps — GPU-Accelerated Kubernetes**

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-FX-16+V1

MODULE – V	**06 Hours**

Cloud DevOps, DevSecOps & Site Reliability Engineering

Topics: Cloud DevOps Fundamentals (Service Models, Cloud CI/CD Services, Deployment Strategies, Cost & FinOps Basics), Advanced Deployment Patterns (Blue-Green, Canary, A/B Testing, Feature Flags, Progressive Delivery), Chaos Engineering (Principles, Chaos Tools, Game Days, Resilience Testing), DevSecOps (SAST, DAST, SCA, Container Scanning, Secrets Detection, Policy as Code), GitOps in Production (ArgoCD, Flux, Repo Structure, Automated Deployment & Rollback), Site Reliability Engineering (SRE Principles, SLIs/SLOs/SLAs, Error Budgets, Incident Management, Toil Reduction)

Applications: Full blue-green deployment on AWS ECS Fargate via CodePipeline with automatic rollback on health-check failure - zero-downtime release, Canary release with Argo Rollouts: 5% → 20% → 50% → 100% traffic progression with automated Prometheus-based analysis and rollback on latency SLO breach

AI Integration: AI-powered cloud cost optimisation recommendations (AWS Compute Optimizer, Google Cloud Recommender, Cast AI Kubernetes rightsizing), Generative AI in incident response: PagerDuty Copilot for LLM-generated alert summaries, runbook lookup, and draft post-mortem narratives.

Authentic Intelligence: Error budgets are a shared contract between product management and engineering - gaming the measurement window undermines the reliability model and ultimately harms users, Chaos engineering in production demands explicit stakeholder consent, defined blast radius, and rollback capability — it is never a surprise exercise

NVIDIA DLI Free Courses (Relevant to this Module):

1. MLOps Fundamentals — Production AI Deployment, Monitoring & Model Governance (8 hrs) | Path: MLOps & DevOps for AI — End-to-End Production AI

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-FX-23+V1

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Explain the DevOps philosophy, CALMS framework, Three Ways, DORA metrics, and design a complete DevOps toolchain map for a given software delivery scenario; write Bash automation scripts for server provisioning and log analysis; implement advanced Git branching strategies for team collaboration.	L2
2	Build production-grade Docker images using multi-stage Dockerfiles with security best practices (non-root, distroless, digest pinning), orchestrate multi-container applications with Docker Compose, and manage container images in a registry with automated vulnerability scanning.	L3
3	Design and implement end-to-end CI/CD pipelines in GitHub Actions and Jenkins integrating automated tests, code quality gates, SAST/SCA security scans, and artifact promotion; provision cloud infrastructure using Terraform modules with remote state; automate configuration management using Ansible roles.	L6
4	Deploy and manage containerised workloads on Kubernetes using Deployments, StatefulSets, Services, Ingress, HPA, RBAC, and Helm charts; configure a full observability stack (Prometheus + Grafana + EFK) with meaningful SLI dashboards and alert routing.	L5
5	Implement DevSecOps security controls (SAST, DAST, SCA, secrets detection, OPA policy gates) in CI/CD pipelines; apply blue-green and canary deployment patterns;	L5

	design SLOs and error budgets; conduct blameless post-mortem analyses; evaluate GitOps and chaos engineering practices for production reliability.	

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	2	2	1	-	2	1	1	2	2	1	2	3	2
CO2	2	2	2	-	3	-	1	2	1	-	2	3	2
CO3	3	3	3	2	3	1	1	3	1	2	2	3	3
CO4	2	3	3	2	3	-	1	2	2	1	2	3	2
CO5	2	3	3	3	3	1	2	2	2	2	3	3	3

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Gene Kim, Jez Humble, Patrick Debois & John Willis - The DevOps Handbook: How to Create World-Class Agility, Reliability, & Security in Technology Organizations, IT Revolution Press, 2nd Edition, 2021
2. Nigel Poulton - Docker Deep Dive, Independently Published, 2023 Edition.

REFERENCE BOOKS:

1. Jez Humble & David Farley - Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation, Addison-Wesley, 2010
2. Brendan Burns, Joe Beda, Kelsey Hightower & Lachlan Evenson - Kubernetes: Up and Running, O'Reilly Media, 3rd Edition, 2022.

RECOMMENDED TOOLS

- Development Environment: VS Code (with Remote-SSH, Docker, Kubernetes extensions) | JetBrains Fleet | Vim/Neovim for terminal workflows
- Version Control: Git 2.40+ | GitHub / GitLab | GitHub Desktop (beginners) | GitKraken (visual Git history)
- Containerisation: Docker Desktop (macOS/Windows) | Podman (rootless alternative, Linux) | Docker Buildx | Trivy / Grype (image scanning) | Hadolint (Dockerfile linting)
- Kubernetes: minikube or kind (local cluster) | kubectl | k9s (TUI cluster manager) | Helm 3 | Lens IDE | k8sGPT (AI diagnostics)
- CI/CD: GitHub Actions | Jenkins (via Docker: jenkins/jenkins:lts) | ArgoCD | Flux CD | Tekton (cloud-native alternative)
- AI Assistants: GitHub Copilot, ChatGPT, Claude

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

DEEP LEARNING

[As per Choice Based Credit System (CBCS) Scheme]

SEMESTER – V

Course Code	:		Credits	:	04
Hours / Week	:	05	Total Hours	:	45+30
L–T–P–J	:	3–0–2–0	CIE + SEE	:	60+40 Marks

Course Vision: To develop the ability to design, analyze, implement, and evaluate deep learning solutions for engineering problems by integrating data-driven modeling, GPU-accelerated computing, and responsible AI practices.

Course Objectives:

This course will enable students:

- To understand the fundamental building blocks of deep learning: neurons, MLPs, activation functions, backpropagation, and optimizers.
- To apply regularization, normalization, and representation learning techniques to build robust deep learning models.
- To design and implement Convolutional Neural Networks (CNNs) for image classification, object detection, and segmentation tasks.
- To develop sequential models (RNN, LSTM, GRU) and Transformer-based architectures for NLP and time-series applications.
- To construct generative models (VAE, GAN), apply one-shot learning, and evaluate models using Explainable AI and Responsible AI principles.

Teaching-Learning Process (General Instructions)

These are sample pedagogical methods teachers can adopt to develop course outcomes:

- Lecture Method: Traditional and interactive delivery methods to develop course outcomes.

- Interactive Teaching: Brainstorming, group discussion, focused listening, formulating questions, and notetaking.
- Video/Animation: Video demos and animations to explain deep learning concepts visually.
- Collaborative Learning: Group-based lab exercises and peer code review.
- Critical Thinking: At least three Higher Order Thinking (HOT) questions per session.
- Different Ways to Solve: Show multiple solutions and encourage student creativity.

MODULE – I- Foundations of Neural Networks & Deep Learning	09 Hours

Topics: History of Deep Learning and AI milestones; McCulloch-Pitts Neuron, Perceptron, Multilayer Perceptrons (MLPs); Activation Functions: Sigmoid, ReLU, Tanh, Softmax; Loss Functions: MSE, Cross-Entropy; Feed Forward Neural Networks; Gradient Descent; Backpropagation Algorithm: chain rule, computational graphs; Optimizers: Batch GD, Stochastic GD, Mini-Batch GD, Momentum, Nesterov Accelerated GD, ADAM.

Applications: Network Intrusion Detection — MLP classifying network traffic (KDD Cup/UNSW-NB15 dataset); Malware Binary

AI Integration: Implementation using Python (NumPy, TensorFlow/Keras) — build and train MLP from scratch; implement backpropagation step-by-step; compare optimizers on MNIST dataset.

Authentic Intelligence: Critical evaluation of architecture.

MODULE – II Regularization, Optimization & Representation Learning	**09 Hours**

Topics: Bias-Variance Tradeoff; L2 Regularization (Weight Decay); Early Stopping; Dataset Augmentation; Dropout and DropConnect; Better Activation Functions: ReLU, ELU, GELU; Batch Normalization; Greedy Layer-wise Pretraining;

Applications: Network Anomaly Detection — Denoising autoencoder on normal traffic; reconstruction error flags zero-day attacks

AI Integration: Implement Dropout and Batch Normalization in a fully connected network using PyTorch; train denoising autoencoder on corrupted MNIST images; visualize latent space of autoencoder; compare Word2Vec embeddings using Gensim.

Authentic Intelligence: Evaluation of bias and tradeoff, strategic planning of augmentmentation techniques

MODULE – III Convolutional Neural Networks & Computer Vision	**09 Hours**

Topics: Convolution Operation: kernels, feature maps, stride, padding; Pooling Layers; Full CNN Architecture; Landmark CNN Models: LeNet-5, AlexNet, ZFNet, VGGNet, GoogLeNet (Inception), ResNet, DenseNet; Transfer Learning: fine-tuning with pre-trained models; Object Localization and Detection: bounding boxes, YOLO variants; Semantic Segmentation: FCN, U-Net; Instance Segmentation: Mask RCNN.

Applications: Malware Visualization — PE binaries converted to grayscale images; ResNet-based malware family classification ;CCTV Threat Detection — CNN for unauthorized access detection at data centres; Network Packet Visualization — flow bytes as 2D arrays.

AI Integration: Build and train CNN on CIFAR-10; visualize filters and feature maps; fine-tune pre-trained ResNet50/VGG16 for a custom classification task (transfer learning); implement YOLO for real-time object detection using OpenCV.

Authentic Intelligence: Strategic planning and evaluation of layers

MODULE – IV Recurrent Neural Networks, Attention & Transformers	**09 Hours**

Topics: Recurrent Neural Networks (RNN): architecture, hidden state; Backpropagation Through Time (BPTT); Vanishing and Exploding Gradients, Gradient Clipping; Truncated BPTT; Gated Recurrent Units (GRU); Long Short-Term Memory (LSTM): cell state, gates; Bidirectional RNNs and LSTMs; Encoder-Decoder (Seq2Seq) Models; Attention Mechanism: self-attention, multi-head attention, positional encoding, Introduction to GNN

Applications: Log Sequence Anomaly Detection — LSTM/GRU on syslog/Windows event-ID sequences to detect APT lateral movement; Threat Intelligence NLP — BERT fine-tuned on CVE/threat reports for automatic IOC extraction;

AI Integration: Implement LSTM for time-series anomaly detection on server log data; build a GRU-based text classifier;

Authentic Intelligence: Diagnosis of gradients, Evaluation of pre trained models

MODULE – V- Generative Models	**09 Hours**

Topics: Autoencoders: encoder-decoder structure, relation to PCA; Regularization in Autoencoders: Denoising Autoencoders, Sparse Autoencoders; Variational Autoencoders (VAE): latent space regularization, reparameterization trick; Generative Adversarial Networks-Introduction;One-Shot & Few-Shot Learning; Explainable AI (XAI) Introduction: why model interpretability matters; Grad-CAM for CNN decisions; LIME / SHAP concept.

Applications: Synthetic Attack Data Generation -GAN augmenting imbalanced IDS training datasets; Zero-Day Detection (One-Shot);

AI Integration: Train a DCGAN on MNIST; apply Grad-CAM to visualize CNN decisions on security images.

Authentic Intelligence: Deep understanding on Latent space, evaluation and interpretation of XAI methods

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Understand the basic building blocks of deep learning — neurons, MLPs, backpropagation, and optimizers — to design feed-forward neural networks.	L2
2	Apply regularization, normalization, and representation learning techniques including autoencoders and word embeddings to build robust deep learning models.	L3
3	Design and implement CNN architectures for image classification, object detection, and segmentation; apply transfer learning to real-world datasets.	L3
4	Develop sequential models (RNN, LSTM, GRU) and Transformer-based architectures for NLP, time-series, and cybersecurity applications.	L3
5	Evaluate and learn generative models (VAE, GAN), apply one-shot learning, and interpret model decisions using Explainable AI methods.	L5

Mapping Levels of COs to POs / PSOs

				Table: Mapping Levels of COs to POs / PSOs									
COs	1	2	3	4	5	6	7	8	9	10	11	PSO 1	PSO 2
CO1	2	2	1	-	-	-	-	-	-	-	1	2	2
CO2	3	2	1	1	1	2	1	-	2	1	1	2	2
CO3	3	2	1	1	1	2	1	-	2	1	1	2	2
CO4	3	2	1	1	1	2	1	-	2	1	1	2	2
CO5	3	2	1	1	1	2	1	-	2	1	1	2	2

3: Substantial (High) 2: Moderate (Medium) 1: Poor (Low)

TEXT BOOKS:

- Deep Learning — Ian Goodfellow, Yoshua Bengio, Aaron Courville. MIT Press, 2016. (Available free at deeplearningbook.org)
- Neural Networks and Deep Learning — Michael Nielsen. Online book, 2015. (neuralnetworksanddeeplearning.com)

REFERENCE BOOKS:

- Pattern Recognition and Machine Learning — Christopher M. Bishop. Springer, 2006.
- Deep Learning with Python — François Chollet. Manning Publications, 2nd Edition, 2021.

RECOMMENDED TOOLS

- Programming: Python (NumPy, Pandas, TensorFlow 2 / Keras, PyTorch) — Google Colab / Jupyter Notebook / Visual Studio Code
- Visualization: Matplotlib, Seaborn, TensorBoard
- Model Deployment: NVIDIA Triton Inference Server, NVIDIA Morpheus, TensorRT
- Cybersecurity Tools: Wireshark, Metasploit (for dataset generation), Elastic SIEM

LAB EXERCISES- 30 HOURS

S.No	Exercise Title	Aim / Objective	Tools	Hrs	CO
1	Perceptron & MLP	Implement a single-layer Perceptron; build and train an MLP on MNIST using NumPy from scratch.	Google Colab / Jupyter	2 h	CO1
2	Activation Functions & Loss	Implement and compare Sigmoid, ReLU, Tanh activation functions; compute MSE and Cross-Entropy loss.	Google Colab / Jupyter	2 h	CO1
3	Optimizers	Implement Gradient Descent, SGD, Mini-Batch GD, Momentum, and Adam; compare convergence on a regression task.	Google Colab / Jupyter	2 h	CO1
4	Dropout & Batch Normalization	Implement Dropout and Batch Normalization in a fully connected network; compare accuracy and overfitting.	Google Colab / Jupyter	2 h	CO2
5	Autoencoder	Build and train an Autoencoder for image reconstruction and anomaly detection on MNIST.	Google Colab / Jupyter	2 h	CO2
6	CNN on CIFAR-10	Design and train a CNN on CIFAR-10; visualize filters and feature maps.	Google Colab / Jupyter	2 h	CO3
7	Transfer Learning	Fine-tune pre-trained VGG16/ResNet50 for a custom image classification task.	Google Colab / Jupyter	2 h	CO3

8	Object Detection	Implement YOLO for real-time object detection using OpenCV on a custom dataset.	Google Colab / Jupyter	2 h	CO3
9	LSTM Time-Series	Implement an LSTM network for time-series prediction (e.g., temperature or network log anomaly data).	Google Colab / Jupyter	2 h	CO4
10	Traffic Analysis with GRU	Apply GRU to classify network traffic logs into benign vs. malware.	Google Colab / Jupyter	2 h	CO4
11	BERT Fine-tuning	CTI report classification into ransomware, phishing and DDoS using BERT	Google Colab / Jupyter	2 h	CO4
12	GAN Training	Train a GAN on MNIST; generate synthetic images and evaluate quality.	Google Colab / Jupyter	2 h	CO5
13	Explainable AI	Apply Grad-CAM to a trained CNN; use SHAP/LIME to explain predictions on a tabular security dataset.	Google Colab / Jupyter	2 h	CO5

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

FORENSIC FUNDAMENTALS

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - V

Course Code		**Credits**	03
Hours / Week	04	**Total Hours**	445
L–T–P–J	3–0–0–0	**CIE+SEE**	60+40 Marks

Course Vision:

To build a basic conceptual, legal, and procedural foundation in digital forensics, enabling students to understand cybercrime, investigation methodology, and evidence handling in alignment with industry standards and legal frameworks, before progressing to specialized professional electives such as Disk & Memory Forensics and Mobile & IoT Forensics.

Course Objectives:

This course will enable students:

1. To provide knowledge of digital forensics concepts, cybercrime classification, and the forensic investigation lifecycle
2. To understand the legal, ethical, and regulatory framework governing digital evidence
3. To develop understanding of standard forensic investigation process models and evidence-handling procedures
4. To analyze forensic considerations across network, cloud, email, web, and social media environments
5. To examine anti-forensic techniques, the forensic tool landscape, and emerging trends in digital forensics

Teaching-Learning Process (General Instructions)
These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:
1. Combination of lecture-based teaching with interactive methods such as brainstorming, group discussions, and question-driven learning to enhance understanding of forensic concepts.
2. Use of case studies and real-world cybercrime scenarios, including frameworks such as NIST and ISO/IEC 27037, to connect theoretical concepts with practical application.
3. Incorporation of multimedia tools such as videos and case documentaries to illustrate investigation processes and legal proceedings.
4. Encouragement of collaborative learning through group activities, mock investigations, and process-model comparison tasks to build teamwork and analytical skills.
5. Promotion of critical thinking through higher-order questions, quizzes, and scenario-based problem solving, enabling students to evaluate forensic investigation approaches.

MODULE – I	**08 Hours**
Introduction to Digital Forensics and Cybercrime Forensic science: definition, history, and branches; digital forensics: definition, evolution, and objectives; distinguishing digital forensics, cyber forensics, and computer forensics; classification of cybercrime; Locard's Exchange Principle in digital contexts; roles and responsibilities of a digital forensic investigator; forensic readiness and organizational preparedness; overview of career paths in digital forensics; case studies of cyber incidents.	
MODULE – II	**08 Hours**
Legal, Ethical, and Regulatory Framework Admissibility of digital evidence: relevance, authenticity, reliability; IT Act 2000 and amendments; Indian Evidence Act – Section 65B (electronic records); Digital Personal Data Protection Act, 2023; GDPR – data protection overview; search and seizure: warrants and constitutional safeguards; chain of custody: concept and documentation; ethics in forensic investigation; expert witness testimony and courtroom procedure; overview of ISO/IEC 27037, 27041/27042.	
MODULE – III	**08 Hours**
Forensic Investigation Process and Evidence Handling Digital forensic investigation lifecycle: identification, preservation, collection, examination, analysis, presentation; process models: NIST, ACPO, SWGDE, Kruse & Heiser (comparative overview); crime scene management and first responder procedures; evidence preservation principles: integrity verification and hashing (conceptual); evidence volatility considerations (conceptual only); forensic report structure and objectivity; quality assurance and validation in examinations.	
MODULE – IV	**08 Hours**

Forensic Perspectives on Networks, Cloud, and Online Communication Network forensics fundamentals: sources of evidence – logs, firewalls, IDS/IPS (conceptual); cloud forensics challenges: multi-tenancy, jurisdiction, data volatility; email forensics: architecture, header analysis fundamentals, phishing indicators; web forensics: browser artifacts overview, web server log basics; social media forensics: evidentiary value and attribution challenges; forensic challenges of encrypted communication (conceptual).	
MODULE – V	**08 Hours**
Anti-Forensics, Tool Landscape, and Emerging Trends Anti-forensic techniques: data hiding, obfuscation, timestamp manipulation, secure deletion (conceptual); steganography: concept and detection challenges; encryption as an anti-forensic and privacy challenge; malware forensics overview: static vs. dynamic analysis (high-level); forensic tool categories: acquisition, analysis, open-source vs. commercial (survey only); emerging trends: AI in forensics, blockchain forensics, big data forensics; professional certifications overview: CHFI, GCFA, CCE; case studies from publicly documented investigations.	

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Understand digital forensic principles, cybercrime classification, and the investigation lifecycle	L2
2	Interpret the legal, ethical, and regulatory requirements governing digital evidence and investigations	L2
3	Apply standard forensic investigation process models and evidence-handling procedures	L3
4	Interpret forensic considerations in network, cloud, email, web, and social media environments	L3
5	Apply anti-forensic techniques, the forensic tool landscape, and emerging trends in digital forensics	L3

Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	3	2	-	-	-	-	-	-	-	-	-	3	2

CO2	3	2	2	-	-	-	-	-	-	-	-	3	2
CO3	2	3	3	2	1	-	-	-	-	-	-	2	3
CO4	2	3	3	3	2	-	-	-	-	-	-	3	2
CO5	2	2	2	3	2	2	-	-	-	-	-	2	3

3: Substantial (High) 2: Moderate (Medium) 1: Poor (Low)

TEXT BOOKS:

1. Nelson, B., Phillips, A., & Steuart, C., Guide to Computer Forensics and Investigations, Cengage Learning (latest edition).
2. Godbole, N., & Belapure, S., Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India, 2013.

REFERENCE BOOKS:

1. Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Academic Press.
2. NIST Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response.
3. ACPO, Good Practice Guide for Digital Evidence.
4. Eoghan Casey (ed.), Handbook of Digital Forensics and Investigation, Academic Press.

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

DATABASE MANAGEMENT SYSTEMS

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - V

Course Code	:		**Credits**	:	04
Hours / Week	:	05	**Total Hours**	:	45+30
L–T–P–J	:	3–0–2–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

To develop the ability to design, implement, optimize, and secure modern database systems by integrating relational foundations with emerging NoSQL and AI-driven data management paradigms.

Course Objectives:

The course aims to enable students to:

1. Build strong foundations in data modelling and relational database design
2. Develop proficiency in SQL for querying and database programming
3. Apply normalization and optimization techniques for efficient databases
4. Understand transaction processing and system reliability mechanisms
5. Explore NoSQL and modern data-driven applications in real-world scenarios

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with traditional lecture method, different types of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I	**09 Hours**

DATABASE FUNDAMENTALS & ER MODEL

Topics: Introduction, Purpose of Database System, Data models, Views of data, Three-schema architecture Components of DBMS, Conceptual data modelling, Entities, entity types, Attributes, relationships, Relationship types, E/R diagram notation, ER diagram Examples

Applications: Enterprise database design (ERP, CRM systems), Banking and financial database modelling, Healthcare information systems (EHR/EMR), E-commerce product and customer data modelling

AI Integration: AI-assisted ER diagram generation from natural language requirements, Automated schema suggestion tools based on domain patterns, Intelligent entity and attribute extraction from unstructured data, AI-based data modelling assistants.

Authentic Intelligence: Identifying correct entities and relationships from real-world scenarios, Resolving ambiguity in requirements during schema design, Deciding appropriate level of abstraction in ER models, Translating business rules into accurate data models.

MODULE – II	**09 Hours**

RELATIONAL MODEL & SQL

Topics: Relational Data Model- Concept of relations, schema-instance distinction, Keys, referential integrity and foreign key, Relational algebra operators, Data definition in SQL, table, key and foreign key definitions, Update behaviors, querying in SQL, querying in SQL, Notion of aggregation, aggregation functions group by and having clauses.

Applications: Business intelligence and reporting systems, Inventory and supply chain management databases, Academic and student information systems, Financial data analysis and reporting

AI Integration: Text-to-SQL tools for automatic query generation, AI-based query optimization and execution planning, Smart SQL assistants for debugging and query correction, Automated indexing recommendations.

Authentic Intelligence: Text-to-SQL tools for automatic query generation, AI-based query optimization and execution planning, Smart SQL assistants for debugging and query correction, Automated indexing recommendations.

MODULE – III	**09 Hours**

DATABASE DESIGN & NORMALIZATION

Topics: Text-to-SQL tools for automatic query generation, AI-based query optimization and execution planning, Smart SQL assistants for debugging and query correction, Automated indexing recommendations.

Applications: Large-scale enterprise database optimization, Data warehouse schema design, Banking and transaction systems ensuring consistency, Healthcare databases minimizing redundancy

AI Integration: AI-driven normalization recommendations, Automated detection of functional dependencies, Intelligent schema optimization tools, Pattern-based database design assistants

Authentic Intelligence: Deciding normalization level vs system performance trade-offs, Identifying hidden dependencies not captured formally, Designing schemas aligned with business workflows, Applying denormalization where necessary for performance.

MODULE – IV	**09 Hours**

TRANSACTION MANAGEMENT & RECOVERY

Topics: Transactions: ACID Properties, Transaction States , Schedules in DBMS , Schedules in DBMS, Locking based protocols for CC, Error recovery and logging, Undo, redo, undo-redo logging , Recovery methods. **Applications:** Banking systems (transaction consistency), Airline reservation systems (concurrent access), E-commerce platforms (order processing systems), Real-time financial systems **AI Integration:** AI-based anomaly detection in transaction patterns, Predictive failure detection and recovery planning, Intelligent deadlock detection mechanisms, Automated log analysis for recovery **Authentic Intelligence:** Interpreting transaction conflicts and resolving inconsistencies, Deciding recovery strategies in critical failures, Prioritizing transactions in high-load systems, Understanding real-world implications of isolation levels.	
MODULE – V	**09 Hours**
NOSQL & MODERN DATABASES **Topics:** Limitations of RDBMS, NoSQL overview: CAP theorem, BASE properties, Types: Key-Value (Redis), Document (MongoDB), Column-family (Cassandra), Graph DB (Neo4j basics) MongoDB: BSON, collections, CRUD operations, Aggregation framework, Indexing, **Applications:** Social media platforms (unstructured data storage), IoT data management systems, Real-time analytics and big data platforms, Content management systems **AI Integration:** AI-based query optimization in NoSQL databases, Automated schema inference for document databases, Intelligent indexing and performance tuning, AI-driven recommendation systems using NoSQL data **Authentic Intelligence:** Choosing between SQL and NoSQL based on application needs, Designing scalable data architectures, Interpreting NoSQL query results and performance behavior, Balancing consistency, availability, and scalability (CAP trade-offs)	

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	**Design** conceptual database schemas using ER modelling and DBMS architecture principles.	L3
2	**Develop** relational queries using SQL and relational algebra for data retrieval and manipulation.	L3
3	**Analyze** and **apply** normalization techniques and functional dependencies for efficient database design.	L4

4	**Evaluate** transaction processing, concurrency control, and recovery mechanisms in DBMS.	L5
5	**Compare** and **implement** NoSQL database models for scalable and distributed applications.	L4

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	3	2	2	–	–	–	–	–	2	2	1	3	2
CO2	3	3	2	–	2	–	–	–	2	2	1	3	2
CO3	3	2	3	–	2	–	–	–	2	2	1	3	3
CO4	2	3	3	–	3	–	–	–	2	2	1	2	3
CO5	2	3	3	–	3	–	–	–	2	2	2	2	3

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Elmasri and Navathe, ”Fundamentals of Database Systems“, Seventh Edition, Pearson Education, 2021, 2015.
2. P. J. Sadalage and M. Fowler, "NoSQL Distilled: A Brief Guide to the Emerging World of Polyglot Persistence", First Edition, Pearson Education, Inc. 2012.

REFERENCE BOOKS:

1. Raghu Ramakrishnan and Johannes Gehrke, “Database Management Systems”, Third Edition, McGraw-Hill, 2003.

LAB EXERCISES- 30 HOURS

S.No	Exercise Title	Aim / Objective	Tools	Hrs	CO
1	**Create a table called Employee & execute the following.** **Employee (EMPNO,ENAME,JOB, MANAGER_NO, SAL, COMMISSION)** **1. Create a user and grant all permissions to the user.** **2. Insert the any three records in the employee table contains attributes EMPNO,** **ENAME JOB, MANAGER_NO, SAL, COMMISSION and use rollback. Check the** **result.** **3. Add primary key constraint and not null constraint to the employee table.** **4. Insert null values to the employee table and verify the result.**	To create an Employee table, practice user management, perform DML operations, and understand constraints like PRIMARY KEY and NOT NULL along with transaction control (ROLLBACK).	Oracle Database / MySQL / PostgreSQL SQL Command Line / SQL Developer	2 h	CO1
2	**Create a table called Employee that contain attributes EMPNO, ENAME,JOB, MGR,SAL** **& execute the following.** **1. Add a column commission with domain to the Employee table.** **2. Insert any five records into the table.** **3. Update the column details of job** **4. Rename the column of Employ table using alter command.** **5. Delete the employee whose Empno is 105**	To perform table modifications using ALTER commands and practice INSERT, UPDATE, DELETE operations on an Employee table.	MySQL Workbench / pgAdmin SQL	2 h	CO2
3	**Queries using aggregate functions(COUNT,AVG,MIN,MAX,SUM),Group by,Orderby.** **Employee(E_id, E_name, Age, Salary)** **1. Create Employee table containing all Records E_id, E_name, Age, Salary.** **2. Count number of employee names from employee table** **3. Find the Maximum age from employee table.** **4. Find the Minimum age from employee table.** **5. Find salaries of employee in Ascending Order.** **6. Find grouped salaries of employees.**	To understand and apply aggregate functions (COUNT, SUM, AVG, MIN, MAX) along with GROUP BY and ORDER BY clauses.	Oracle Database / MySQL SQL Interface	2 h	CO2
4	**Create a row level trigger for the customers table that would fire for INSERT or UPDATE** **or DELETE operations performed on the CUSTOMERS table. This trigger will display the** **salary difference between the old & new Salary.** **CUSTOMERS(ID,NAME,AGE,ADDRESS,SALARY)**	To create and implement row-level triggers to monitor INSERT, UPDATE, and DELETE operations and track salary changes.	Oracle Database / PostgreSQL PL/SQL or SQL	2 h	CO2

5	**Create cursor for Employee table & extract the values from the table. Declare the variables** **,Open the cursor & extract the values from the cursor. Close the cursor.** **Employee(E_id, E_name, Age, Salary)**	To understand cursor operations for row-by-row processing of query results in a database.	Oracle Database PL/SQL	2 h	**CO3**
6	**Install an Open Source NoSQL Database MongoDB & perform basic CRUD(Create, Read,** **Update & Delete) operations. Execute MongoDB basic Queries using CRUD operations.**	To install and use a NoSQL database and perform basic CRUD operations.	MongoDB MongoDB Compass / Mongo Shell	2 h	**CO3**
	Open Ended Questions				
8	**E-Commerce Database Design** **You are building a database for a large e-commerce platform like Amazon.** **The system must handle millions of users, orders, products, and reviews.** **Question:** • **How would you design the database schema to ensure scalability and performance? Discuss:** • **Table structure and relationships** • **Indexing strategies** • **Handling high transaction volumes** • **Trade-offs between normalization and denormalization**	To design a scalable and efficient database schema for a large-scale e-commerce system handling high transaction volumes.	MySQL / PostgreSQL ER Diagram Tools (e.g., Lucidchart)	2 h	**CO4-CO5**
9	**Banking System Consistency** **A bank similar to State Bank of India needs to ensure that money transfers between accounts are always accurate, even during system failures.** **Question:** **How would you use DBMS concepts to guarantee data consistency and reliability? Explain:** • **Use of transactions and ACID properties** • **Concurrency control methods** • **Recovery mechanisms in case of crashes**	To understand and implement DBMS concepts like ACID properties, concurrency control, and recovery mechanisms for reliable transactions.	Oracle Database PL/SQL / SQL	2 h	**CO4-CO5**
10	**Social Media Platform Scaling** **A social media app like Instagram stores posts, likes, comments, and follower relationships.** **Question:** **How would you design the database to efficiently handle:** • **Real-time feed generation**	To design a database capable of handling large-scale data, real-time operations, and distributed storage for social media applications.	MongoDB / Cassandra System Design Tools (e.g., Draw.io)	2 h	**CO5**

	• **Massive read/write operations** • **Data partitioning or sharding strategies**				

2. Silberschatz, Korth and Sudharshan: "Database System Concepts", Seventh Edition, McGrawHill, 2019.
3. Date, A. Kannan, S. Swamynatham: "An Introduction to Database Systems", Eight Edition, Pearson Education, 2012.

RECOMMENDED TOOLS

Databases:

- MySQL / PostgreSQL
- MongoDB Atlas
- Firebase

Programming:

- Python (SQLite, PyMongo)
- Node.js

AI Tools:

- ChatGPT / GitHub Copilot
- DataRobot / H2O.ai

Visualization:

- Power BI / Tableau

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

AI-DRIVEN HARDWARE SECURITY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - V

Course Code	:		**Credits**	:	03
Hours / Week	:	03	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

To develop the ability to analyze, design, and secure hardware systems using artificial intelligence techniques, enabling protection against modern hardware-level threats in embedded and computing platforms.

Course Objectives:

This course will enable students:

1. To understand the fundamentals of hardware security and various hardware-based attack models.
2. To learn cryptographic hardware implementations and security primitives such as PUFs and TRNGs.
3. To analyze side-channel and fault attacks and understand their impact on hardware systems.
4. To apply artificial intelligence techniques for detecting hardware vulnerabilities, anomalies, and attacks.
5. To design and evaluate secure hardware systems using AI-driven approaches for real-world cybersecurity applications.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. Use lecture methods supported with visual aids to explain hardware security concepts and attack models.
2. Demonstrate hardware attacks and countermeasures using development boards and simulation tools.
3. Encourage hands-on learning through lab experiments on side-channel analysis and fault injection.
4. Integrate real-world case studies of hardware security vulnerabilities and mitigation techniques.
5. Introduce basic AI/ML tools for analyzing hardware security data and anomaly detection.
6. Promote mini-projects and problem-based learning on AI-driven hardware security applications.

MODULE – I	**09 Hours**

Foundations of AI-Driven Hardware Security

Topics: Introduction to hardware security and threat landscape, hardware attack models (side-channel, fault, Trojans, reverse engineering), hardware security in IC lifecycle, basics of embedded and FPGA systems, introduction to data-driven security concepts, role of AI in hardware vulnerability analysis and threat detection.

Applications: Smart devices, secure embedded systems, critical infrastructure protection.

Authentic Intelligence: Understanding challenges in applying AI to hardware systems due to limited data, noise, and resource constraints.

MODULE – II	**09 Hours**

AI-Assisted Cryptographic Hardware & Security Primitives

Topics: Overview of hardware implementation of cryptographic algorithms (AES, RSA, ECC), Physically Unclonable Functions (PUFs) and TRNGs, security metrics (reliability, uniqueness), AI-based modeling and analysis of PUF behavior, machine learning techniques for randomness evaluation and hardware authentication.

Applications: Secure authentication, key generation, device identity systems.

Authentic Intelligence: Understanding limitations of AI models in accurately predicting hardware randomness and security behavior.

MODULE – III	**09 Hours**

AI-Enhanced Side-Channel & Fault Analysis

Topics: Side-channel attacks: power analysis (SPA, DPA basics), timing and cache attacks, electromagnetic leakage, fault injection techniques, differential fault analysis concepts, use of machine learning for side-channel signal classification, pattern recognition in power traces, automated attack detection.

Applications: Security testing of embedded devices, smart cards, and cryptographic hardware.

Authentic Intelligence: Understanding noise, data variability, and real-world challenges in AI-based attack analysis.

MODULE – IV	**09 Hours**

AI-Based Hardware Trojan Detection & Anti-Tamper Techniques

Topics: Hardware Trojan taxonomy and insertion, detection techniques (functional and side-channel), IC counterfeiting and IP piracy, reverse engineering threats, AI-based anomaly detection in circuits, machine learning approaches for Trojan detection, anti-tamper techniques (logic locking, obfuscation).

Applications: Trusted IC design, secure manufacturing, IP protection.

Authentic Intelligence: Understanding limitations of AI in detecting stealthy Trojans and challenges in large-scale hardware analysis.

MODULE – V	**09 Hours**

Secure Hardware Systems with AI-Based Monitoring

Topics: Secure boot and root of trust, trusted execution environments (ARM TrustZone), firmware security, hardware security modules (HSMs), microarchitectural vulnerabilities (Spectre, Meltdown basics), AI-based monitoring of hardware systems, anomaly detection in runtime behavior, predictive security mechanisms.

Applications: Secure embedded platforms, cloud hardware security, automotive systems.

Authentic Intelligence: Understanding trade-offs between security, performance, and AI deployment in hardware systems.

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Describe hardware security concepts, threat models, and attack types in computing systems.	L2
2	Explain cryptographic hardware implementations and security primitives such as PUFs and TRNGs.	L2
3	Analyze side-channel and fault attacks on embedded and hardware systems.	L3
4	Apply AI/ML techniques for detecting hardware vulnerabilities and anomalies.	L3
5	Evaluate and develop secure hardware systems using AI-driven approaches for real-world applications.	L5

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	3	2	2	1	-	-	-	-	-	-	1	2	2
CO2	3	2	2	1	2	-	-	-	-	-	1	2	2
CO3	3	3	2	2	2	-	-	-	1	1	1	2	3

CO4	2	3	3	2	3	1	1	2	2	1	1	2	3
CO5	2	3	3	2	3	2	1	2	2	1	1	2	3

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. 1. Sarup Bhunia and Mark Tehranipoor, Hardware Security: A Hands-on Learning Approach, Elsevier, 2019.
2. Debdeep Mukhopadhyay and Rajat Subhra Chakraborty, Hardware Security: Design, Threats, and Safeguards, CRC Press, 2014.

REFERENCE BOOKS:

1. Ahmad-Reza Sadeghi and David Naccache (Eds.), Towards Hardware-Intrinsic Security: Foundations and Practice, Springer, 2010.
2. Ian Goodfellow, Yoshua Bengio, and Aaron Courville, Deep Learning, MIT Press, 2016.
3. Aurélien Géron, Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow, 2nd Edition, O'Reilly, 2019.

RECOMMENDED TOOLS

- **Programming Languages:** Python, Embedded C
- **Development Platforms**: SRM Cortex-M), FPGA (Xilinx/Intel), ESP32 / Arduino
- **Hardware Security Tools**: ChipWhisperer, Oscilloscope, Logic Analyzer
- **Hardware Interface Tools**: OpenOCD, JTAGulator
- **Firmware Analysis Tools:** Binwalk, Firmware Analysis Toolkit (FACT)
- **Protocol Analysis Tools:** Wireshark, bettercap
- **Hardware Security Assessment Tools:** CHIPSEC
- **Simulation & Design Tools:** Xilinx Vivado / Intel Quartus
- **AI/ML Tools:** Python (NumPy, Pandas, Scikit-learn, TensorFlow, PyTorch)
  Communication Tools: PuTTY, Tera Term

CRIMINAL PSYCHOLOGY AND BEHAVIORAL INTELLIGENCE

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - V

Course Code	:		**Credits**	:	03
Hours / Week	:	03	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

To develop a deep understanding of criminal behavior, psychological profiling, and behavioral intelligence techniques to analyze, predict, and prevent criminal activities using scientific, ethical, and analytical approaches.

Course Objectives:

This course will enable students:

1. Understand the psychological foundations of criminal behavior.
2. Analyze criminal patterns using behavioral and cognitive theories.
3. Apply profiling techniques to identify and predict criminal tendencies.
4. Integrate behavioral intelligence with modern investigative systems.
5. Develop ethical awareness in handling criminal and psychological data.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. Lecture method along with interactive teaching techniques.
2. Brainstorming, discussions, and case-based learning.
3. Use of crime case studies and behavioral analysis scenarios.
4. Encouraging critical thinking and ethical reasoning.
5. Analytical exercises and simulation-based learning.

MODULE – I	**09 Hours**

Foundational Perspectives in Criminal Psychology

Topics: Definition and scope of criminal psychology, nature of crime, types of criminals, psychological vs sociological perspectives, criminal behavior theories (biological, psychological, social), factors influencing crime (environmental, genetic, cultural), introduction to behavioral intelligence, fundamentals of digital and social media behavior analysis.

Applications: Crime pattern understanding, law enforcement analysis, criminal classification, social crime prevention.

AI Integration: Crime data classification, Pattern recognition in criminal records, Predictive policing models

Authentic Intelligence: Understanding human motives, Ethical analysis of criminal intent, avoiding bias in criminal judgment

MODULE – II	**09 Hours**

Theories of Criminal Behaviour

Topics: Classical and positivist theories, psychoanalytic theory (Freud), behavioral theory, cognitive theory, social learning theory, personality disorders and crime, mental illness and criminality, psychology of online behavior and cyber aggression, influence of social media on criminal behavior and radicalization.

Applications: Psychological evaluation of offenders, legal decision support, risk assessment of individuals, rehabilitation planning.

AI Integration: Behavioral pattern modeling, risk prediction systems, psychological profiling tools, sentiment analysis in social media platforms.

Authentic Intelligence: Ethical diagnosis of mental conditions, avoiding misinterpretation of behavior, human-centered analysis.

MODULE – III	**09 Hours**

Criminal Profiling and Behavioural Analysis

Topics: Criminal profiling techniques, offender profiling models (FBI approach), geographic profiling, victimology, modus operandi vs signature behavior, forensic psychology basics, interrogation psychology, digital footprint analysis, social media profile analysis in criminal investigations.

Applications: Serial offender identification, crime scene analysis, investigation support systems, suspect narrowing.

AI Integration: Pattern recognition in crime data, facial and behavior analysis systems, profiling using machine learning, social media analytics for criminal investigations.

Authentic Intelligence: Responsible use of profiling, avoiding stereotyping, ethical interrogation practices.

MODULE – IV	**09 Hours**

Behavioural Intelligence in Crime Prevention

Topics: Behavioral intelligence concepts, decision-making patterns in criminals, deception detection, body language analysis, lie detection techniques, cyber behavior analysis, threat assessment, social media content analysis, online threat monitoring, misinformation and extremist content identification.

Applications: Security and surveillance systems, fraud detection, insider threat analysis, cybercrime behavior tracking, social media intelligence systems.

AI Integration: Emotion detection systems, behavioral biometrics, AI-based surveillance analytics, sentiment and trend analysis in social media data.

Authentic Intelligence: Privacy and ethical surveillance, responsible interpretation of behavior, human oversight in AI systems. .

MODULE – V	**09 Hours**

Cyber Terrorism, Radicalization, and Emerging Cyber Threats

Topics: Psychology of terrorism, organized crime behavior, cybercriminal psychology, radicalization processes, criminal rehabilitation, criminal justice system psychology, psychology of online extremism, future trends in behavioral intelligence and AI-assisted crime prediction.

Applications: Counter-terrorism strategies, cybercrime investigation, criminal rehabilitation programs, national security planning.

AI Integration: Predictive threat intelligence, deep learning for behavior prediction, automated crime detection systems, AI-driven social media monitoring systems.

Authentic Intelligence: Ethical AI in law enforcement, balancing surveillance and rights, responsible policy making.

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
CO1	Explain the concepts, theories, and factors influencing criminal behaviour and behavioural intelligence.	L2
CO2	Apply psychological and behavioural analysis techniques in criminal investigation and offender assessment.	L3
CO3	Analyze criminal profiling methods, crime patterns, cyber behaviour, and social media content in investigative contexts.	L4

CO4	Evaluate behavioural intelligence techniques for crime prevention, threat assessment, and security applications.	L4
CO5	Assess the role of AI-assisted behavioural analytics and ethical practices in modern criminal psychology and security systems.	L4

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	3	2	1	-	-	-	2	-	-	-	1	2	1
CO2	3	3	2	2	2	-	2	-	-	-	1	3	2
CO3	3	3	3	2	3	-	2	-	-	-	1	3	3
CO4	2	3	2	2	3	-	3	-	-	-	1	3	2
CO5	2	2	3	2	3	-	3	-	-	-	2	3	3

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Curt R. Bartol & Anne M. Bartol – Criminal Behavior: A Psychological Approach, Pearson
2. David Canter – Criminal Psychology: A Beginner's Guide, Oneworld Publications
3. Wayne Petherick – Profiling and Serial Crime, Academic Press

REFERENCE BOOKS:

1. James W. Osterburg & Richard H. Ward – Criminal Investigation: A Method for Reconstructing the Past
2. Richard N. Kocsis – Criminal Profiling: Principles and Practice
3. Adrian Raine – The Anatomy of Violence

MINI PROJECTS

Students will design a behavioral intelligence system such as:

- Criminal profiling system
- Crime prediction model
- Fraud behavior detection tool

- Cybercriminal behavior analysis system
- Threat assessment dashboard

RECOMMENDED TOOLS

- Python
- Pandas
- NumPy
- Scikit-learn
- Tableau / Power BI
- Jupyter Notebook

APPLICATION SECURITY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER: V

Subject Code		**Credits**	**03**
Hours/Week	**03 Hours**	**Total Hours**	**45 Hours**
L-T-P-S	**3-0-0-0**		

Course Learning Objectives:

This course will enable students to:

1. Understand the principles and practices of secure programming.
2. Identify and mitigate security risks in web applications.
3. Apply security measures to protect applications from common threats and attacks.
4. Explore advanced topics and applications of security in various contexts.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking,*** ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps

improve the student's understanding.

UNIT- I	09 Hours

Introduction to Application Security

Overview of Application Security, Importance and Need for Application Security, - Secure Software Development Lifecycle (SDLC), Secure Requirements Gathering and Analysis, Secure Design Principles, Code Review and Testing for Security.

UNIT- II	09 Hours

WEB AND MOBILE APPLICATION SECURITY

INTRODUCTION, LET'S HACK A WEBSITE, HOW BROWSERS WORK, HOW THE INTERNET WORKS, HOW WEB SERVERS WORK, HOW PROGRAMMERS WORK, SESSION HIJACKING, INFORMATION LEAKS, ENCRYPTION, XML ATTACKS, DON'T BE AN ACCESSORY, DENIAL-OF-SERVICE ATTACKS, INJECTION ATTACKS, THIRD-PARTY CODE, CROSS-SITE SCRIPTING ATTACKS, CROSS-SITE REQUEST FORGERY ATTACKS, COMPROMISING AUTHENTICATION, MOBILE EXPLOITS AND MALWARE, IOS SECURITY MODEL, ANDROID SECURITY MODEL, COMPARING PERMISSION MODELS, WI-FI SECURITY: EVIL TWIN, JASAGER,SSLSTRIP.

UNIT- III	10 Hours

PROMPT ENGINEERING SECURITY:

THE POWER OF PROMPT ENGINEERING, FINE-TUNING THE PROMPT WITH TECHNIQUES, PROMPTING FOR TEXT GENERATION, PROMPTING FOR QUESTION ANSWERING, PROMPTING FOR CODE GENERATION, EVALUATING AND TESTING PROMPTS, ETHICAL CONSIDERATIONS IN PROMPT ENGINEERING, SECURITY AND PRIVACY PRESERVING PROMPT ENGINEERING-ISSUES AND CHALLENGES.

UNIT-IV	10 Hours

SUPPLY CHAIN SECURITY

INTRODUCTION, BENEFITS OF INVESTING IN SUPPLY CHAIN SECURITY, SUPPLY CHAIN SECURITY MANAGEMENT, MEASURING THE VALUE CREATED BY SUPPLY CHAIN SECURITY, ISO **28000** AND SIX SIGMA, FIVE STEPS OF THE SIX SIGMA PROJECT (DMAIC), OVERVIEW OF CONTEMPORARY SUPPLY CHAIN SECURITY INITIATIVES, SUPPLY CHAIN SECURITY TECHNOLOGIES & THEIR APPLICATIONS: SMART CONTAINERS, TRACKING SYSTEMS, BAR CODE & RFID TAGS, INTRUSION DETECTION SENSORS, ACCESS POINTS, FENCING, IDENTITY MANAGEMENT SYSTEMS (IDMS), ELECTRONIC ACCESS CONTROL SYSTEM (EACS), VEHICLE ELECTRONIC ACCESS CONTROL SYSTEM (VEACS), CONTAINER DETECTION AND SCREENING EQUIPMENT.

UNIT-V	07Hours

API SECURITY

UNDERSTANDING APIS- GROWING THE API ECONOMY- SECURING APIS WITH TRADITIONAL APPROACHES- MODERN APPROACHES TO SECURING APIS- BENEFITTING FROM AN API SECURITY FRAMEWORK: AUTOMATING YOUR API SECURITY FRAMEWORK- DEVOPS AND DEVSECOPS.

Course Outcomes:

Atthe end of the course, the student will be able to:

1. Apply secure programming practices to develop robust and secure applications
2. Identify vulnerabilities and implement security measures in web applications
3. Understand and implement security throughout the software development lifecycle
4. Explore advanced topics and applications of security in various domains
5. Analyze and evaluate emerging trends and technologies in application security

COs \ POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	3	2	-	-	-	-	-	-	-	-	-	2	-
CO2	3	3	1	-	-	-	-	-	-	-	-	3	-
CO3	2	3	3	2	1	-	-	-	-	-	-	3	2
CO4	2	3	3	2	2	-	-	-	-	-	-	3	2
CO5	2	2	3	2	3	-	-	-	-	-	-	3	3

TEXTBOOKS:

1. Web Application Hacker's Handbook: Finding and Exploiting Security Flaws by Dafydd Stuttard and Marcus Pinto.
2. API Security for Dummies by Emily Freeman, John Wiley & Sons Inc., 2020.
3. Supply Chain Security Management, Initiatives & Technologies, Thomas Miller, First Edition, 2010.
4. Prompt Engineering Playbook by GovTech Data Science & AI Division, 2023.

REFERENCE BOOKS:

1. "OWASP Testing Guide v4" by OWASP Foundation, 2014.
2. **"Mobile Application Security:** Protecting Mobile Devices and Their Applications" by Himanshu Dwivedi, Chris Clark, and David Thiel, 2012.
3. **"Building Secure and Reliable Systems:** Best Practices for Designing, Implementing, and Maintaining Systems" by Heather Adkins, Betsy Beyer, Paul Blankinship, and Ana Oprea.
4. **Secure Coding:** Principles and Practices by Mark G. Graff and Kenneth R. van Wyk.

ONLINE RESOURCES

1. https://www.ncsc.gov.uk/collection/supply-chain-security
2. https://project.linuxfoundation.org/hubfs/CNCF SSCP vl.pdf
3. https://www.developer.tech.gov.sg/products /collections /data-science-and-artificial-intelligence /playbooks /prompt-engineering-playbook-beta-v3.pdf
4. https://terrorgum.com/tfox/books/security_engineerin a guide_to building_dependable_distributed_ systems.pdf
5. https://datasciencehorizons.com/pub/Masterin Generative AI Prompt_Engineerin Data Science Ho rizons v2.pdf
6. https://arxiv.org/pdf/2404.06001
7. https://www.cybertalk.org/wp-content/uploads_/2_024/04_/The-cyber-security-professionals-guide-to-prompt-engineerin_.pdf
8. https://owasp.org/www-project-mobile-app-security/
9. https: //www.itu.int/en/ITU-D /Regional-Presence /AsiaPacific /SiteAssets /Pages /Events /2019 /ITUPITA2018 /ITU-ASP-CoE-Training-on-/Mobile%2 0Apps%2 0Security_fv.pdf
10. https://www.dhs.gov/sites/default/files/publications/2019 mobilesecurity_rd_programguide_vol3.pdf

Activity Based Learning (Suggested Activities in Class)

1. Hands-on coding exercises to implement secure programming practices
2. Web application vulnerability assessment and remediation exercises.
3. Case studies and group discussions on real-world security incidents and solutions

****

Course Title: Cyber Law, Ethics, and Governance

Course Code:
Credits: 3
Semester:
Programs: B.Tech. CSE (Cyber Security)

Prerequisite:

Course Type: Professional Elective

Course Vision

To develop legally aware, ethically responsible, and governance-oriented cybersecurity professionals capable of addressing digital risks, ensuring compliance, and applying AI-driven technologies within legal and ethical frameworks.

Course Objectives

The course aims to enable students to:

1. **Understand cyber laws and legal frameworks** governing digital systems, cybercrime, and data protection.
2. **Analyze ethical issues in cyberspace** including privacy, surveillance, intellectual property, and professional conduct.
3. **Apply governance models and regulatory standards** for cybersecurity risk management and compliance.
4. **Evaluate cybercrime investigation processes** and digital evidence handling procedures.
5. **Assess emerging challenges** in AI, data governance, and global cyber regulations.

Course Outcomes

CO No	Description
CO1	Understand cyber laws, cybercrime types, and ethical principles
CO2	Apply legal frameworks including IT Act and global regulations
CO3	Analyze ethical, privacy, and intellectual property issues
CO4	Evaluate cyber governance, risk, and compliance frameworks
CO5	Apply digital forensic and investigation techniques within legal boundaries

UNIT – I: Foundations of Cyber Law and Cyber Ethics

Topics
Introduction to Cyber Law: Need, Scope, Evolution, Cybercrime: Types (hacking, phishing, identity theft, cyber terrorism), Legal terminology: Jurisdiction, liability, evidence, Ethics in cyberspace: Professional ethics, cyber ethics principles, Privacy and surveillance issues, Overview of Indian Cyber Law (IT Act 2000 & Amendments)

Applications

- Cybercrime awareness systems
- Legal compliance in IT organizations
- Ethical decision-making frameworks

AI Tools

- AI-based legal research assistants
- NLP tools for cyber law document analysis
- AI-driven compliance monitoring systems

Authentic Intelligence (AI)

- Ethical responsibility in digital actions
- Balancing privacy vs surveillance
- Legal accountability in cyber activities

UNIT – II: Information Technology Act & Cyber Regulations

Topics

Detailed study of IT Act 2000 and IT (Amendment) Act 2008, Digital signatures and electronic governance, Cyber offenses and penalties, Role of adjudicating officers and cyber appellate tribunal, International cyber laws (GDPR overview, global frameworks), Data protection and privacy laws.

Applications

- E-governance systems
- Digital authentication and secure transactions
- Legal compliance auditing

AI Integration

- AI-based compliance verification systems
- Smart contract validation tools
- Automated legal risk assessment

Authentic Intelligence

- Responsible use of digital identity systems
- Ethical handling of personal data
- Legal transparency in automated systems

UNIT – III: Cyber Ethics, Privacy, and Intellectual Property

Topics

Ethical theories in cybersecurity (Utilitarianism, Deontology), Intellectual Property Rights (IPR): Copyright, patents, trademarks, Software piracy and digital rights management, Data privacy principles and frameworks, Ethical hacking vs illegal hacking, social media ethics and digital behaviour.

Applications

- Software licensing systems
- Digital rights management platforms
- Privacy-preserving systems

AI Integration

- AI-based plagiarism detection
- Privacy-preserving ML (federated learning basics)
- AI for content moderation

Authentic Intelligence

- Ethical AI usage and bias mitigation
- Respect for intellectual property
- Responsible digital citizenship

UNIT – IV: Cyber Governance, Risk, and Compliance

Topics

Cyber governance frameworks (ISO 27001, NIST), Enterprise Risk Management (ERM) in cybersecurity, Security policies, standards, and procedures, Incident response and cyber resilience, Role of regulatory bodies and CERT organizations, Cyber audit and compliance mechanisms.

Applications

- Organizational cybersecurity governance
- Risk assessment and mitigation systems
- Incident response planning

AI Integration

- AI-based risk prediction models
- Security analytics platforms
- Automated compliance dashboards

Authentic Intelligence

- Accountability in governance decisions
- Transparency in risk reporting
- Ethical leadership in cybersecurity

UNIT – V: Digital Forensics, Cyber Investigation & Emerging Trends

Topics

Digital evidence: Collection, preservation, chain of custody, Cybercrime investigation process, Role of forensic tools and expert witnesses, Legal admissibility of digital evidence, AI, blockchain, and cyber law challenges, Emerging trends: Cyber warfare, AI regulations

Applications

- Digital forensic investigations

- Law enforcement cyber units
- Cybersecurity policy development.

AI Integration

- AI-based forensic analysis tools
- Automated log and evidence analysis
- Blockchain for evidence integrity

Authentic Intelligence

- Ethical investigation practices
- Avoiding misuse of surveillance technologies
- Ensuring fairness in AI-driven legal systems
-

CO \ PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	3	2	-	1	-	-	-	3	-	-	-	1	1
CO2	3	3	2	2	2	-	-	3	-	-	-	2	2
CO3	2	3	2	2	-	-	-	3	1	-	-	2	2
CO4	3	3	3	3	3	1	-	3	1	1	-	3	3
CO5	3	3	3	3	2	1	-	3	1	1	-	3	3

MINI PROJECT THEMES

Students will design an AI-based model to solve real-world problems.

- Analysis of a real cybercrime case under IT Act
- Data breach investigation and legal implications
- GDPR compliance evaluation of an organization
- Ethical analysis of AI surveillance systems
- AI-based cybercrime detection system
- Privacy risk assessment tool
- Cyber law compliance auditing system
- Digital evidence management system

Recommended Tools

Technical Tools

- Python (for analysis & AI models)
- Wireshark (network forensics)
- Autopsy / Sleuth Kit (digital forensics)

AI & Data Tools

- Scikit-learn
- Pandas, NumPy
- NLP tools (for legal document analysis)

Legal & Governance Tools

- Online legal databases (Manupatra, SCC Online)
- Compliance tools (ISO frameworks, risk tools)
- Documentation tools (MS Word, LaTeX)

TEXT BOOKS:

1. Cyber Security, Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Sunit Belapure and Nina Godbole, Wiley Publications
2. Cyber Law: The Law of the Internet, Jonathan Rosenoer, Springer Verlag, New York, Berlin, Heidelberg
3. CYBER LAW by Dr Pavan Duggal - Latest Third Edition - Universal LexisNexis Original

REFERENCE BOOKS:

1. Computer Law: Chris Reed & John Angel Oxford University Press
2. Cybersecurity, Cybercrime and Cyberlaw, Paul Bocij et al.
3. Principles of Information Security, Michael E. Whitman & Herbert J. Mattord
4. Cyber Law, Ethics, and Privacy: A Comprehensive Guide, Illuminate Code Labs
5. Cybersecurity and Cyberlaw, Dr. J.P. Mishra
6. Cyber Security and Cyber Laws, Nilakshi Jain & Ramesh Menon Khanna Publishers

COMPUTER VISION FUNDAMENTALS **[As per Choice Based Credit System (CBCS) Scheme]** **SEMESTER – V**					
Course Code	:		Credits	:	03

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

Hours / Week	:	03	Total Hours	:	45
L–T–P–J	:	3–0–0–0	CIE + SEE	:	60+40 Marks

Course Vision: To equip students with a strong conceptual and hands-on foundation in Computer Vision covering classical image processing, feature extraction, segmentation, motion analysis, and applied CV for industrial and cybersecurity domains — enabling them to design, evaluate, and responsibly deploy vision-based AI systems in real-world applications.

Course Objectives: This course will enable students:

- Understand the principles of digital image formation, low-level processing, and spatial/frequency domain filtering.
- Apply classical feature extraction techniques — SIFT, HOG, Harris, RANSAC — and geometric vision concepts including stereo and 3D reconstruction.
- Implement image segmentation methods such as Graph-Cut, Mean-Shift, and MRF-based approaches. Analyse motion in video sequences using optical flow, background subtraction, and the KLT tracker.
- Apply computer vision techniques to real-world cybersecurity problems including image forensics, malware visualisation, deepfake detection, and CCTV-based anomaly detection.
- Appreciate ethical considerations — surveillance bias, privacy, and responsible deployment of vision AI systems.

MODULE – I: Image Formation & Low-Level Processing	09 Hours

Topics: Overview and state-of-the-art in computer vision; digital image formation fundamentals; pixel neighbourhood and connectivity; geometric transformations — Orthogonal, Euclidean, Affine, Projective; Fourier Transform, convolution and spatial filtering in spatial and spectral domains; image enhancement and restoration; histogram processing and equalisation; morphological operations — dilation, erosion, opening, closing.

Applications: Image forensics — detecting tampered or forged document images using histogram analysis; steganalysis — detecting hidden data embedded in images using spatial frequency analysis; CAPTCHA generation and break-resistance analysis using morphological distortions.

AI Integration: Implement Fourier filtering, morphological operations, and histogram equalisation using OpenCV on Google Colab; apply steganalysis by analysing LSB (Least Significant Bit) patterns in a sample image to detect hidden payloads.

MODULE – II: Feature Extraction & Geometric Vision	**09 Hours**

Topics: Edge detection — Canny, LoG, DoG; Hough Transform for line and shape detection; corner detectors — Harris and Hessian Affine; Scale-Space Analysis — Image Pyramids, Gaussian derivatives; local feature descriptors — SIFT, SURF, HOG, GLOH; Gabor Filters and Discrete Wavelet

Transform (DWT); perspective geometry; binocular stereopsis; camera and epipolar geometry; homography, rectification, DLT, RANSAC; 3D reconstruction framework; auto-calibration.

Applications: Face liveness detection using LBP/HOG texture features to defeat spoofing attacks; copy-move forgery detection in images using SIFT feature matching to locate duplicated regions; detecting deepfake video frames using facial landmark geometric inconsistencies.

AI Integration: Implement Harris corner detection and SIFT feature matching using OpenCV on Google Colab; build a copy-move forgery detector by clustering SIFT keypoints on a test image; visualise epipolar lines and fundamental matrix on a stereo image pair.

MODULE – III: Image Segmentation	**09 Hours**

Topics: Region growing and edge-based segmentation; Graph-Cut segmentation; Mean-Shift clustering for image segmentation; Markov Random Fields (MRFs) for pixel labelling; texture segmentation using Gabor filter banks; watershed segmentation; introduction to semantic and instance segmentation concepts; evaluation metrics for segmentation — IoU, Dice coefficient.

Applications : Malware visualisation — converting binary executables to grayscale images and segmenting structural regions to classify malware families; CCTV crowd segmentation for perimeter intrusion detection; network traffic anomaly visualisation using image-based flow representations and region segmentation.

AI Integration: Implement Graph-Cut and Mean-Shift segmentation on colour images using OpenCV and scikit-image on Google Colab; convert a sample binary file to a grayscale image and apply segmentation to identify structural regions — demonstrating the malware visualisation technique used in cybersecurity research.

MODULE – IV: Motion Analysis & Shape from X	**09 Hours**

Topics: Background subtraction and adaptive background modelling; optical flow — Horn-Schunck and Lucas-Kanade methods; KLT feature tracker; spatio-temporal analysis; dynamic stereo and motion parameter estimation; Shape from X — Phong reflectance model, reflectance map, albedo estimation; photometric stereo; shape from texture, colour, motion, and edges; surface smoothness constraint.

Applications: Abnormal behaviour detection in CCTV using optical flow to flag loitering, tailgating, and perimeter breach; gait recognition using temporal motion features for biometric access control; detecting screen-recording exfiltration by analysing subtle pixel-level motion patterns on monitored endpoints.

AI Integration: Implement Lucas-Kanade optical flow on a CCTV video clip using OpenCV on Google Colab to detect loitering behaviour; perform adaptive background subtraction using MOG2 and flag moving intrusions; implement photometric stereo on a three-image set under different illuminations.

MODULE – V: Applied CV, Adversarial Threats & AI Cybersecurity Pipelines	**09 Hours**

Topics: Visual inspection pipeline — defect detection and quality control; synthetic data generation for CV model training; data augmentation strategies for vision datasets; model deployment basics — TensorRT and NVIDIA DeepStream for edge inference; adversarial attacks on CV models — FGSM, PGD, and adversarial patch attacks; adversarial robustness and defence strategies; CV-based anomaly detection for cybersecurity — digital fingerprinting and behavioural profiling using NVIDIA Morpheus; deepfake detection techniques; ethical and responsible CV — surveillance bias, privacy, and facial recognition regulation.

Applications : Adversarial patch attacks on surveillance cameras to evade person detection systems; using NVIDIA Morpheus digital fingerprinting for visual log anomaly detection and zero-trust profiling; deepfake face detection in video-based identity authentication pipelines; AI-powered CCTV intrusion detection with real-time alerting using NVIDIA DeepStream.

AI Integration: Generate an FGSM adversarial example on an image classifier using PyTorch and measure accuracy drop; build a visual anomaly detection pipeline using NVIDIA Morpheus digital fingerprinting concepts on Google Colab; deploy a TensorRT-optimised CV model for edge inference and benchmark latency vs. standard PyTorch.

Course Outcome

CO	At the end of the course the student will be able to:	Bloom's Taxonomy Level
1	Explain the principles of digital image formation, apply spatial/frequency domain filtering, morphological operations, and connect these to image forensics and steganalysis in cybersecurity.	L2
2	Apply classical feature extraction techniques — Harris, SIFT, HOG, RANSAC — and geometric vision concepts including stereo and 3D reconstruction, with applications in forgery detection and face spoofing defence.	L3
3	Implement image segmentation methods including Graph-Cut, Mean-Shift, and MRF-based approaches, and apply them to malware visualisation and CCTV-based intrusion detection.	L3
4	Analyse motion in video sequences using optical flow, background subtraction, and the KLT tracker, and apply these to cybersecurity scenarios such as CCTV anomaly detection and gait recognition.	L3
5	Discuss adversarial attacks on CV models, build a basic anomaly detection pipeline using NVIDIA Morpheus, and evaluate ethical considerations including surveillance bias and responsible deployment of vision AI.	L2

Table: Mapping Levels of COs to POs / PSOs

COs	1	2	3	4	5	6	7	8	9	10	11	PSO 1	PSO 2
CO1	3	2	1	-	-	2	-	-	2	-	1	2	2
CO2	3	3	2	1	-	2	1	-	2	-	1	2	2
CO3	3	3	2	2	1	2	1	1	2	1	1	3	2
CO4	3	2	2	2	1	2	1	1	2	1	1	2	3
CO5	2	2	1	1	2	3	2	1	3	1	2	2	2

TEXT BOOKS:

- Szeliski, R. (2011). Computer Vision: Algorithms and Applications. Springer-Verlag London Limited.

- Forsyth, D.A. & Ponce, J. (2003). Computer Vision: A Modern Approach. Pearson Education.

- Gonzalez, R.C. & Woods, R.E. (1992). Digital Image Processing. Addison-Wesley.

- IIT Madras CS6350 Computer Vision — Course Handout & Lecture Slides (Prof. V.P. Lab, 2025). cse.iitm.ac.in/~vplab/computer_vision.html

REFERENCE BOOKS:

- Hartley, R. & Zisserman, A. (2004). Multiple View Geometry in Computer Vision (2nd ed.). Cambridge University Press.

- Bishop, C.M. (2006). Pattern Recognition and Machine Learning. Springer.

- Fukunaga, K. (1990). Introduction to Statistical Pattern Recognition (2nd ed.). Academic Press.

- Goodfellow, I. et al. (2014). Explaining and Harnessing Adversarial Examples. arXiv:1412.6572.

RECOMMENDED TOOLS & FRAMEWORKS

- OpenCV (cv2) — image processing, feature extraction, stereo vision, and optical flow (opencv.org)

- scikit-image — segmentation, morphology, and image analysis in Python

- PyTorch / torchvision — adversarial attack generation (FGSM, PGD) and model evaluation

- NVIDIA Morpheus — AI cybersecurity framework for anomaly detection and digital fingerprinting (developer.nvidia.com/morpheus-cybersecurity)

- NVIDIA DeepStream SDK — real-time video analytics and CCTV intrusion detection pipeline

- NVIDIA TensorRT — high-performance deep learning inference for edge CV deployment

- Programming: Python 3 (NumPy, Matplotlib, scikit-learn) — Google Colab / Jupyter (NVIDIA GPU-enabled)

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

ADVERSARIAL MACHINE LEARNING [As per Choice Based Credit System (CBCS) Scheme] **SEMESTER – VI**					
Course Code	:		Credits	:	03
Hours / Week	:	03	Total Hours	:	45
L–T–P–J	:	3–0–0–0	CIE + SEE	:	60+40 Marks
Course Vision: To build foundational awareness of how machine learning systems can be attacked and how to defend them — without requiring advanced mathematics — so that students can recognise adversarial threats in real-world AI applications and apply practical, tool-based countermeasures responsibly.					
Course Objectives: This course will enable students:					

- Understand what adversarial machine learning is and why ML systems are vulnerable to manipulation. Recognise the main types of attacks on ML systems — poisoning, evasion, and privacy attacks — through real-world examples.
- Explore how attackers manipulate training data and test inputs to mislead ML models, using case studies on spam, malware, and network traffic.
- Understand common defences against adversarial attacks and how they protect ML systems in practice.
- Apply beginner-friendly tools (IBM ART, Foolbox, NVIDIA DLI notebooks) to observe adversarial attacks and defences hands-on.

Teaching-Learning Process (General Instructions)

- Lecture Method: Concept-first teaching using diagrams, analogies, and real-world news stories about AI failures.
- Interactive Teaching: Live demos of adversarial attacks using pre-built notebooks; group discussion on real incidents.
- No-Math First Approach: Each concept introduced visually before any formulas are shown.
- Case Study Method: Each module anchored to a real-world attack scenario (spam, malware, facial recognition, chatbots).
- Hands-On Coding: Simple Python notebooks using IBM ART and Foolbox on Google Colab — no GPU required for basic exercises.

MODULE – I: What is Adversarial Machine Learning?	09 Hours

Topics: Adversarial ML- Introduction, Background and Notation-Basic Notation, Statistical Machine Learning, A framework for secure learning-Analyzing the phases of learning, Security Analysis, Framework, Exploratory Attacks, Causative Attacks, Repeated Learning Games, Privacy Preserving Learning

Applications (Cybersecurity): Anti-virus classifier bypassed by slightly modifying a malware file; network intrusion detector evaded by disguising attack traffic as normal; phishing URL classifier fooled by small character substitutions in the URL.

AI Integration: NVIDIA DLI Generative AI Explained video on how AI models work identify three real-world AI systems that could be targets of adversarial attacks;

Textbook References: Book 1: Joseph et al. (2019). Ch. 1 (Introduction), Ch. 2 (ML Background — conceptual sections only). Book 2: Vorobeychik & Kantarcioglu (2018). Ch. 1 (Introduction), Ch. 2 (ML Preliminaries — overview only).

NVIDIA DLI Courses (Relevant to this Module):

1. Getting Started with Deep Learning

   https://courses.nvidia.com/courses/course-v1:DLI+S-FX-01+V1/

2. Generative AI Explained

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-FX-07+V1

MODULE – II: Training-Time Attacks — Poisoning ML Systems	09 Hours

Topics: Data poisoning attacks- Model poisoning attacks-Poisoning attacks on binary classification: Label flipping attacks, Poison Insertion attack on Kernel SVM, Poisoning attacks on unsupervised learning , Attacks at decision time: Examples of Evasion attacks on ML Models-Attacks on Anomaly detection, Attacks on PDF Malware Classifiers, Modelling decision Time attacks, Whitebox Decision timing attacks, Blackbox decision timing attacks

Applications (Cybersecurity): Label-flipping attack on a phishing URL classifier — flipping phishing URLs to benign in training data; backdoor attack on a malware detector; slowly poisoning a SIEM anomaly detector by injecting crafted logs to raise the normal baseline.

AI Integration: Use a pre-built Google Colab notebook to train a simple text classifier on a small email dataset; inject poisoned samples (spam emails labelled as ham) into the training set and retrain

Textbook References: Book 1: Joseph et al. (2019). Ch. 5 (SpamBayes Case Study — conceptual reading), Ch. 6 (PCA Anomaly Detector Case Study — conceptual reading). Book 2: Vorobeychik & Kantarcioglu (2018). Ch. 5 (Data Poisoning Attacks — introductory sections).

NVIDIA DLI Courses (Relevant to this Module):

1. Exploring Adversarial Machine Learning

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-03+V1

2. Applications of AI for Anomaly Detection

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+C-TC-01+V1

MODULE – III: Defending against Attacks	09 Hours

Topics: Hardening Supervised Learning against Decision Time attacks, Optimal Evasion-Robust Classification, Hardening classifiers against Decision time attacks, Evasion Robustness through Feature level protection, Decision Randomisation, Evasion Robust Regression.

Applications (Cybersecurity): Crafting a malware file with tiny changes so it evades a deep learning anti-virus scanner; manipulating network packet headers to evade a machine learning intrusion detection system; probing a fraud detection API to discover which transactions it flags.

AI Integration: Run a Foolbox or IBM ART notebook on Google Colab: load a pre-trained image classifier, generate a simple adversarial example using a one-line attack function, and visualise the original vs. adversarial image side by side; measure how confidence scores change; test whether the adversarial image also fools a different pre-trained model (transferability experiment) — no GPU required.

Textbook References: Book 1: Joseph et al. (2019). Ch. 7 (Privacy-Preserving Mechanisms — concept only), Ch. 8 (Near-Optimal Evasion — case study reading, skip proofs). Book 2: Vorobeychik & Kantarcioglu (2018). Ch. 4 (Attacks at Decision Time — introductory and example sections).

NVIDIA DLI Courses (Relevant to this Module):

1. Exploring Adversarial Machine Learning

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-03+V1

2. Introduction to Federated Learning with NVIDIA FLARE

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-FX-28+V1

MODULE – IV: Adversarial Attacks on Deep Learning	09 Hours

Topics: Neural Network Models, Attacks on Deep Neural Networks: Adversarial Examples on Image classification models-PGD Attack-FGSM attacks-Examples, Adversarial training as a defence- Other simple defences: input smoothing, JPEG compression, adding noise before prediction- how do we measure if a model is robust? Clean accuracy vs. adversarial accuracy.

Applications (Cybersecurity): FGSM attack on a deep learning malware image classifier (PE binaries visualised as images) — tiny pixel change causes misclassification from malware to benign; adversarial patch attack on a CCTV-based intruder detection system in a data centre.

AI Integration: Run a pre-built Google Colab notebook (IBM ART or Foolbox): apply FGSM to a trained CNN on CIFAR-10; visualise clean vs. adversarial images; measure clean accuracy vs. adversarial accuracy; apply JPEG compression as a simple pre-processing defence and re-measure accuracy; use the NVIDIA DLI Adversarial ML notebook for a guided end-to-end walkthrough on a cloud GPU.

Textbook References: Book 1: Joseph et al. (2019). Ch. 9 (Future Directions — deep learning vulnerability discussion, conceptual reading). Book 2: Vorobeychik & Kantarcioglu (2018). Ch. 7 (Attacking and Defending Deep Learning — conceptual and example sections, skip formal proofs).

NVIDIA DLI Courses (Relevant to this Module):

1. Exploring Adversarial Machine Learning

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-03+V1

2. Fundamentals of Deep Learning

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+C-FX-01+V3

MODULE – V: Defences, Responsible AI & Emerging Threats	09 Hours

Topics: Input preprocessing (deep learning attacks); Membership inference attacks; Model stealing attacks ;Adversarial attacks on Large Language Models (LLMs) — prompt injection: tricking a chatbot to ignore its instructions; Jailbreaking — bypassing safety filters in AI assistants using clever input phrasing; Introduction to MITRE ATLAS — a map of adversarial ML attacks in the real world (like

MITRE ATT&CK but for AI); Responsible AI and adversarial ML — bias amplification under attack; fairness and safety considerations.

Applications (Cybersecurity): Prompt injection attack on a cybersecurity AI assistant (LLM-based SOC tool) to bypass threat analysis rules; model stealing attack against a deployed malware classification API — copying the model for free; using MITRE ATLAS to map adversarial ML techniques to real threat actor behaviour; NVIDIA Morpheus detecting unusual query patterns that indicate a model stealing attempt.

AI Integration: Explore the MITRE ATLAS website (atlas.mitre.org) and map at least three attack techniques from this course to real-world incidents listed in the ATLAS case studies; try a prompt injection experiment on a publicly available LLM demo and document the result.

Textbook References: Book 1: Joseph et al. (2019). Ch. 9 (Open Problems and Future Directions — accessible reading for awareness). Book 2: Vorobeychik & Kantarcioglu (2018). Ch. 8 (The Road Ahead — full chapter, written for general audience).

NVIDIA DLI Courses (Relevant to this Module):

1. Building RAG Agents with LLMs

https://courses.nvidia.com/courses/course-v1:DLI+S-FX-15+V1/

Course Outcome		
CO	**At the end of the course the student will be able to:**	**Bloom's Taxonomy Level**
1	Explain what adversarial machine learning is, identify the main types of attacks on ML systems, and recognise real-world examples of adversarial threats in AI applications.	L2
2	Describe how data poisoning attacks work using case studies (SpamBayes, anomaly detectors), identify signs of poisoned training data, and apply basic data sanitisation as a defence.	L2
3	Demonstrate evasion attacks on a deployed ML model using beginner tools (Foolbox / IBM ART), explain the concept of transferability, and describe how model probing can leak information.	L3
4	Generate adversarial examples using FGSM on a deep neural network, compare clean vs. adversarial accuracy, and evaluate simple defences such as adversarial training and input preprocessing.	L3
5	Identify emerging adversarial threats to LLMs (prompt injection, jailbreaking, model stealing), map attacks to MITRE ATLAS, and apply responsible AI principles to adversarial ML scenarios.	L3

Mapping Levels of COs to POs / PSO													
COs	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**PSO 1**	**PSO 2**
CO1	2	2	1	-	1	2	1	-	2	1	1	2	1
CO2	3	2	1	1	1	2	1	-	2	1	1	2	2
CO3	3	2	2	1	1	2	1	1	2	1	1	2	2
CO4	3	3	2	1	1	2	1	1	2	1	1	2	2
CO5	2	2	1	1	2	3	2	1	3	2	2	2	3

3: Substantial (High) 2: Moderate (Medium) 1: Poor (Low)

TEXT BOOKS:

1. Joseph, A.D., Nelson, B., Rubinstein, B.I.P. & Tygar, J.D. (2019). Adversarial Machine Learning. Cambridge University Press. (ISBN: 978-1-107-04346-6)

Chapters used: 1 (Introduction), 2 (ML Background — overview), 5 (SpamBayes Case Study), 6 (PCA Anomaly Detector), 7 (Privacy — concept), 8 (Evasion — case study), 9 (Future Directions).

2. Vorobeychik, Y. & Kantarcioglu, M. (2018). Adversarial Machine Learning. Morgan & Claypool / Springer. (ISBN: 978-3-031-01580-9)

Chapters used: 1 (Introduction), 2 (ML Preliminaries - overview), 4 (Decision-Time Attacks - concept), 5 (Data Poisoning - intro), 6 (Deep Learning Attacks - concept), 7 (The Road Ahead).

REFERENCE BOOKS:

- Goodfellow, I. et al. (2014). Explaining and Harnessing Adversarial Examples. arXiv:1412.6572. (Free — the paper that introduced FGSM, written accessibly)
- MITRE ATLAS: Adversarial Threat Landscape for AI Systems. (atlas.mitre.org) — free, browser-based, no prior knowledge required
- NIST AI Risk Management Framework (AI RMF 1.0). NIST, 2023. (nvlpubs.nist.gov) — free PDF

RECOMMENDED TOOLS & FRAMEWORKS

- IBM Adversarial Robustness Toolbox (ART) — beginner-friendly Python library; pre-built attack and defence notebooks available (adversarial-robustness-toolbox.readthedocs.io)

- Foolbox — simple Python library for generating adversarial examples in 2–3 lines of code (foolbox.readthedocs.io)

- NVIDIA Morpheus — cybersecurity AI pipeline for detecting adversarial queries (developer.nvidia.com/morpheus-cybersecurity)

- NVIDIA NeMo Guardrails — beginner-friendly LLM defence against prompt injection (developer.nvidia.com/nemo-guardrails)

- MITRE ATLAS — adversarial ML attack map with real-world case studies (atlas.mitre.org)

- Programming: Python 3 (scikit-learn, PyTorch basics) — Google Colab (no GPU required for basic exercises)

LAB EXERCISES-30 HOURS

S.No	Exercise Title	Aim / Objective	Tools	Hrs	CO
1	ML Classifier & Decision Boundary	Train a baseline classifier (SVM/RF) on NSL-KDD; visualize decision boundary; demonstrate simple perturbation on a trained model.	Google Colab / Python / scikit-learn	2 h	CO1
2	Attack Taxonomy Survey	Implement and categorize attacks (white-box vs. black-box, evasion vs. poisoning) on a MNIST model; measure accuracy degradation.	Google Colab / PyTorch	2 h	CO1
3	Threat Modelling Exercise	Map threat models (attacker goals, knowledge, capabilities) to real-world AI security incidents using MITRE ATLAS framework.	Jupyter / MITRE ATLAS	2 h	CO1
4	FGSM & PGD Attack	Implement FGSM and PGD attacks on an image classifier using ART; measure L2/L∞ perturbation norms; visualize adversarial examples.	Google Colab / IBM ART / PyTorch	2 h	CO2
5	Closed-Box Evasion & Transfer	Implement black-box evasion via transferability from surrogate model; compare attack success rates across models.	Google Colab / ART / TextAttack	2 h	CO2
6	Evasion Evaluation with Optuna	Use Optuna to optimize attack hyperparameters (epsilon, steps, step size); plot attack success rate vs. perturbation budget curves.	Google Colab / Optuna / ART	2 h	CO2
7	Model Extraction via API Queries	Query a black-box classification API; train a surrogate model; compare surrogate vs. oracle accuracy and decision boundaries.	Google Colab / PyTorch / Flask	2 h	CO3

8	Model Inversion with AIRT	Use AIRT tools to reconstruct approximate training data representations from model confidence outputs; evaluate reconstruction quality.	Google Colab / AIRT / PyTorch	2 h	**CO3**
9	Membership Inference Attack	Implement shadow model membership inference; measure precision/recall of attack on train vs. test data.	Google Colab / scikit-learn	2 h	**CO3**
10	Backdoor Poisoning Attack	Implement a trigger-based backdoor (BadNet) on CIFAR-10; measure backdoor success rate vs. clean accuracy trade-off.	Google Colab / PyTorch	2 h	**CO4**
11	Witches' Brew Poisoning	Implement gradient-alignment based targeted poisoning (Witches' Brew); compare with label-flipping; evaluate defence with spectral signatures.	Google Colab / PyTorch	2 h	**CO4**
12	Adversarial Training Defence	Apply adversarial training (PGD-AT) to a classifier; measure certified robustness; benchmark clean and robust accuracy.	Google Colab / ART / PyTorch	2 h	**CO4**
13	Prompt Injection Attack	Exploit a vulnerable LangChain LLMMathChain via direct prompt injection to achieve remote code execution; implement defences.	Google Colab / LangChain / Python	2 h	**CO5**
14	LLM Poisoning & Data Extraction	Fine-tune GPT-2 on a trigger-poisoned Alpaca dataset using PEFT; then apply perplexity/compression scoring to extract memorized training data.	Google Colab / HuggingFace / PEFT	2 h	**CO5**
15	AI Red Team Case Study	Design a complete AI red team report for a given ML system: threat model, attack surface, attack execution, defence recommendations, and ethical analysis.	Jupyter / MITRE ATLAS / OWASP	2 h	**CO5**

Operating Systems

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VI

Course Code	:		**Credits**	:	03
Hours / Week	:	3	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

To equip students with industry-relevant skills in developing and deploying modern Operating System concepts by integrating foundational concepts of operating systems in the digital economy.

Course Objectives:

This course will enable students:

1. To understand the basic concepts and functions of operating systems.
2. To understand Processes and Threads
3. To analyze Scheduling algorithms.
4. To understand the concept of Deadlocks.
5. To analyze various Memory and Virtual memory management, File system and storage techniques.
6. To discuss the goals and principles of protection in a modern computer system.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. Lecture method means it includes not only the traditional lecture method but a different types of teaching method that may be adopted to develop the course outcomes.
2. Interactive Teaching: Adopt Active learning that includes brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Show Video/animation films to explain the functioning of various concepts.
4. Encourage Collaborative (Group Learning) Learning in the class.
5. To make Critical thinking, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every concept can be applied to the real world - and when that's possible, it helps improve the student's understanding.

MODULE – I	8 Hours

Introduction to Operating System

Topics: Introduction to operating systems, System structures: What operating systems do?; Computer System organization; Computer System architecture; Operating System structure; Operating System operations; Process management; Memory management; Storage management; Protection and Security; Distributed system; Computing environments. Operating System Services: User - Operating System interface; System calls; Types of system calls; System programs; Operating system design and implementation; Operating System structure; Virtual machines.

Applications: Operating System operations; Process management; Memory management; Storage management; Protection and Security

AI Integration: Use machine learning models to predict process burst time and priority,Use ML models to forecast memory needs of applications,

Authentic Intelligence:

- Machine Learning Models: Regression, Decision Trees, Neural Networks
- Reinforcement Learning (for scheduling)
- Python-based frameworks (TensorFlow, PyTorch)
- OS-level simulation tools (e.g., Linux kernel modules)

NVIDIA DLI Courses (Relevant to this Module):

1. Getting Started with Deep Learning (8 hrs) | Path: Deep Learning — Foundational Deep Learning methods for scheduling

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+C-FX-01+V3

2. Building Real-World AI Applications with NVIDIA NIM (2 hrs) | Path: Generative AI — Deploying LLM Microservices for simulations python based frameworks

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-NIM-01+V1

MODULE – II	10 Hours

Process Management:

Topics: Process Management: Process concept; Process scheduling; Operations on processes. Multi-threaded Programming: Overview; Multithreading models; Threading issues. Process Scheduling: Basic concepts; Scheduling Criteria; Scheduling Algorithms

Applications: Implementation of process scheduling, multithreading and scheduling algorithms

AI Integration: AI-assisted (GitHub Copilot, Tabnine), AI-powered code review for detecting scheduling algorithms

Authentic Intelligence: To test the performance of algorithms in real life examples using AI tools

Nvidia DLICOurse(Relevant to this module)

1. https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+C-AC-01+V1

MODULE – III	9 Hours

Process Coordination

Topics: Process Synchronization: The critical section problem; Peterson's solution; Synchronization hardware; Semaphores; Classical problems of synchronization; Monitors. Deadlocks: Deadlocks; System model; Deadlock characterization; Methods for handling deadlocks; Deadlock prevention; Deadlock avoidance; Deadlock detection and recovery from deadlock.

Applications: Process synchronization and deadlock concepts are applied in OS kernels, databases, cloud computing, and distributed systems to manage concurrency, ensure consistency, avoid conflicts, and maintain efficient, reliable resource allocation.

AI Integration: AI integrates by predicting deadlocks, optimizing scheduling, and detecting anomalies using tools like TensorFlow, PyTorch, and Scikit-learn, enabling adaptive synchronization, intelligent resource allocation, and proactive deadlock avoidance.

Authentic Intelligence: Authentication intelligence enhances secure synchronization using anomaly detection, behavioral biometrics, and access control with tools like Okta, Azure AD, and IBM Security Verify, preventing unauthorized access and ensuring system integrity.

NVIDIA DLI Free Courses (Relevant to this Module):

1. **Building Conversational AI Applications** (8 hrs) | Path: Conversational AI — Integrating LLM APIs via Node.js REST Back-Ends

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-FX-17+V1

MODULE – IV	9 Hours

Memory Management

Topics: Memory Management Strategies: Background; Swapping; Contiguous memory allocation; Paging; Structure of page table; Segmentation. Virtual Memory Management: Background; Demand paging; Copy-on-write; Page replacement; Allocation of frames; Thrashing

Applications: Memory management and virtual memory techniques are used in operating systems, cloud platforms, and virtualization to optimize RAM usage, enable multitasking, improve performance, and support efficient execution of large applications.

AI Integration: AI enhances memory management by predicting page faults, optimizing replacement strategies, and detecting thrashing using tools like TensorFlow, PyTorch, and Scikit-learn, improving allocation efficiency and overall system performance.

Authentic Intelligence: Authentication intelligence secures memory access using anomaly detection, access control, and encryption with tools like Okta, Azure AD, and IBM Security Verify, preventing unauthorized access and ensuring data protection.

NVIDIA DLI Courses (Relevant to this Module):

1. https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+C-AC-02+V1

MODULE – V	9 Hours

File System and Secondary Storage Structure

Topics: File System, Implementation of File System: File system: File concept; Access methods; Directory structure; File system mounting; File sharing. Protection: Implementing File system: File system structure; File system implementation; Directory implementation; Allocation methods; Free space management. Mass storage structures; Disk structure; Disk attachment; Disk scheduling; Disk management; Swap space management. Protection and Security: Protection: Goals of protection, Principles of protection, System Security: The Security Problem, Program Threats, System and Network Threats.

Applications: File systems and storage structures manage data organization, access, sharing, and protection in operating systems, databases, and cloud environments, ensuring efficient storage utilization, reliable disk management, and secure system operations.

AI Integration: AI enhances file systems by predicting disk usage, optimizing scheduling, detecting anomalies, and automating organization using tools like TensorFlow, PyTorch, Splunk, and Elasticsearch for intelligent, efficient storage management.

Authentic Intelligence: Authentication intelligence secures file systems through identity verification, access control, and threat detection using tools like Okta, Azure AD, IBM Security Verify, and RSA SecurID, ensuring protection against unauthorized access.

NVIDIA DLI Free Courses (Relevant to this Module):

1. https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+C-FX-01+V3

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course, the student will be able to:		
1	Summarize the basic concepts of operating systems and identify their variants.	L2
2	Apply the FIFO, SJF, SRT, Priority, and Round Robin algorithms to solve process scheduling problems.	L3
3	Summarize process coordination and apply Banker's algorithm to prevent inter-process deadlock.	L2
4	Distinguish between contiguous and virtual memory management.	L3
5	Apply the page replacement algorithms to detect page faults that appear in virtual memory.	L3
6	Apply FCFS, SSTF, SCAN, C-SCAN, Look and C-Look algorithms to solve I/O scheduling.	L3

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs-		
COs	**Program Outcomes (POs)**	**PSOs**

	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	3			-	-	-	-	-	-	-	-	1	-
CO2	1	3	2	-	-	-	-	-	-	-	-	2	-
CO3		3	2	-	-	-	-	-	-	-	1	2	-
CO4	3				-	-	-	-	-	-	-	1	-
CO5		2	3	-	1	-	-	-	-	-	-	1	-
CO6	1	2	3	-	-	-	-	-	-	-	-	1	-

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, Operating System Principles 8th edition, WileyIndia, 2010.

REFERENCES:

1. Operating Systems-Internals and Design Principles, William Stallings, 6th Edition, Pearson Education, 2009.

2. Operating Systems: A Modern Perspective, Gary J. Nutt, Addison-Wesley, 1997.

E-Resource:

1. https://onlinecourses.nptel.ac.in/noc24_cs80/preview

2. https://onlinecourses.nptel.ac.in/noc24_cs108/preview

3. https://www.coursera.org/learn/codio-intro-to-operating-systems-2-memory-management

4. Modern Operating Systems by Andrew S. Tanenbaum - Known for its comprehensive coverage of modern operating systems principles and design.

5. Operating System Fundamentals - Course (nptel.ac.in)

6. Introduction to Operating Systems - Course (nptel.ac.in)

7. Intro to Operating Systems 1: Virtualization | Coursera

8. Intro to Operating Systems 3: Concurrency | Coursera

9. Intro to Operating Systems 2: Memory Management | Coursera

Activity Based Learning (Suggested Activities in Class)

1. Implementing Operating System concepts by doing Mini projects.

2. Case study to compare various Operating Systems and their performance.

3. Present real-world case studies or problems related to operating systems design and performance optimization, encouraging students to apply theoretical knowledge to analyze and propose solutions.

RECOMMENDED TOOLS

- Dev Tools: Visual Studio Code, Git & GitHub
- Deployment: Vercel / Netlify (frontend), Render / AWS (backend)
- AI Assistants: GitHub Copilot, ChatGPT, Claude

VULNERABILITY ANALYSIS AND PENETRATION TESTING [As per Choice Based Credit System (CBCS) scheme] SEMESTER–VI			
Subject Code :		Credits :	03
Hours / Week :	03 Hours 60Hours	Total Hours :	
L–T–P–J :	3–0–2–0		

Course Learning Objectives:

This Course will enable students to:

1. Understand the evolving tools, tactics and procedures used by cybercriminals to breach networks.
2. Discuss implications of common vulnerabilities and recommend ways to rectify or mitigate.
3. More complex vulnerabilities are sought which cannot be found by automated scanners and the effectiveness of the security measures taken at the technical, organizational and personnel level is checked.
4. Understand the legal aspects, industry ethics and the approaches and methodologies used when performing a penetration test.
5. Be able to use the appropriate penetration testing tools for a given scenario and understand their output.

Teaching-Learning Process (General Instructions)
These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes.

1. Lecture method means it includes not only traditional lecture method, but different type of teaching methods may be adopted to develop the course outcomes.
2. Interactive Teaching: Adopt the Active learning that includes brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and roleplaying.
3. Show Video/animation films to explain functioning of various concepts.
4. Encourage Collaborative (Group Learning) Learning in the class.
5. To make Critical thinking, ask at least three Higher order Thinking questions in the class.
6. Adopt Problem Based Learning, which osters students' Analytical skills, develop thinking skills such as the ability to evaluate, generalize, and analyse information rather than simply recall it.
7. Show the different ways to solve the same problem and encourage the students to come up with their own creative ways to solve them.
8. Discuss how every concept can be applied to the real world - and when that's possible, it helps improve the students' understanding.

Course Outcome	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Summarize the significance o risk, security and vulnerability assessment.	L2
2	Analyze penetration testing strategies or diagnosing security o web application using OWASP standards.	L4
3	Identiy the types o vulnerability assessment policies to evaluate system security.	L5
4	Apply modern tools and techniques like Metasploit, RouterSploit, Backdoor, remote access to gather active and passive inormation o a system.	L3
5	Apply web application security concepts to design application portolio or reducing risk and vulnerabilities.	L3

MODULE 1	8Hrs

Vulnerability Management Governance: Security basics, Identification, Authentication, Authorization, Auditing, Accounting, Non–repudiation, Vulnerability, Threats, Exposure, Risk, Safeguards, Attack vectors. Understanding the need for security assessments: Types of security tests: Security testing, Vulnerability assessment versus penetration testing, Security assessment, Security audit.	
MODULE 2	7Hrs
Penetration testing standards, Penetration testing lifecycle, industry standard, Open Web Application Security Project (OWASP) testing guide. Security Assessment Prerequisites: Target scoping and planning, Gathering requirements: checklist of test requirements, time frame and testing hours, Identifying stakeholders.	
MODULE 3	8Hrs
Types of vulnerability assessment: based on location, based on knowledge about environment/ infrastructure, Announced and Unannounced Automated Testing, Manual Testing Estimating the resources and deliverables, Preparing a test plan, Getting approval and signing NDAs, Confidentiality and Nondisclosure Agreements.	
MODULE 4	9Hrs
Information Gathering: Passive information gathering, Active information gathering. Enumeration: Enumeration Services. Gaining Network Access: Gaining remote access, Cracking passwords, Creating backdoors using Backdoor Factory, Exploiting remote services using Metasploit, Hacking embedded devices using RouterSploit, Social engineering using SET.	
MODULE 5	7Hrs
Assessing Web Application Security: Importance of web application security testing, Application profiling, Common web application security testing tools, Authentication, Authorization, Session management, Input validation, Security misconfiguration.	

TEXT BOOKS:

1. Sagar Rahalkar, Network Vulnerability Assessment, Packt Publishing Inc, 2018.

REFERENCE BOOKS:

1. Abhishek Singh, Baibhav Singh and Hirosh Joseph, Vulnerability Analysis and Deense or the Internet, Springer Publishing Inc, 2008.
2. Wil Allsopp, Unauthorized Access: Physical Penetration Testing For IT Security, Wiley Publishing Inc, 2009.
3. Kimberly Graves, Vulnerability Analysis and Deense or the Internet, Wiley Publishing Inc.; 2007.
4. Shakeel Ali and Tedi Heriyanto, Backtrack -4: Assuring security by penetration testing", PACKT Publishing; 2011

****

CYBER RISK MANAGEMENT

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VI

Course Code	:		**Credits**	:	02
Hours / Week	:	02	**Total Hours**	:	30
L–T–P–J	:	2–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

To develop professionals capable of identifying, analyzing, and managing cyber risks in complex digital environments by applying structured risk management frameworks, security controls, and governance practices aligned with industry standards. .

Course Objectives:

This course will enable students:

1. To provide knowledge of cyber risk concepts, threats, and vulnerabilities
2. To develop skills in risk assessment and analysis techniques
3. To understand industry-standard risk management frameworks
4. To apply risk mitigation strategies and security controls
5. To analyze governance, compliance, and emerging cyber risks

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. Combination of lecture-based teaching with interactive methods such as brainstorming, group discussions, and question-driven learning to enhance understanding of cyber risk concepts.
2. Use of case studies and real-world scenarios, including frameworks like NIST and ISO/IEC 27005, to connect theoretical concepts with practical applications.
3. Incorporation of multimedia tools such as videos and animations to demonstrate cyber attacks, risk assessment processes, and security control mechanisms.
4. Encouragement of collaborative learning through group activities, risk analysis exercises, and framework comparison tasks to build teamwork and analytical skills.
5. Promotion of critical thinking through higher-order questions, quizzes, and scenario-based problem solving, enabling students to design and evaluate cyber risk mitigation strategies.

MODULE – I	**06 Hours**

Introduction to Cyber Risk - Cyber risk fundamentals, risk, threat and vulnerability concepts, attack surface, threat actors and motivation, cyber kill chain, attack vectors, risk management lifecycle, cybersecurity principles, security posture, risk appetite and tolerance, enterprise risk vs cyber risk, digital transformation risks, case studies of cyber incidents.

……

Application: Application of cyber risk management in enterprise sectors such as banking, healthcare, and critical infrastructure.

AI Integration: Use of AI for threat detection, anomaly identification, and attack pattern recognition.

Authentic Intelligence: Use of real-time threat intelligence feeds, security reports, and incident databases.

MODULE – II	**06 Hours**

Risk Assessment and Analysis - Asset identification and classification, data classification, business impact analysis, threat intelligence, threat modeling methodologies, vulnerability assessment, penetration testing concepts, qualitative and quantitative risk analysis, likelihood and impact estimation, risk scoring models, risk matrix, attack trees, risk register, exposure analysis, scenario-based risk assessment.

……

Application: Application of risk assessment techniques for asset evaluation, vulnerability analysis, and risk prioritization.

AI Integration: AI-driven risk assessment, predictive analytics, and automated risk scoring models.

Authentic Intelligence: Utilization of CVE databases, vulnerability repositories, and threat intelligence platforms

MODULE – III	**04 Hours**

Risk Management Frameworks - NIST Risk Management Framework, NIST Cybersecurity Framework, ISO/IEC 27005, ISO/IEC 27001 controls, FAIR model, OCTAVE framework, COBIT framework, CIS Critical Security Controls, framework comparison and implementation strategies.

……

Application: Application of frameworks like NIST and ISO/IEC 27005 for structured risk management.

AI Integration: Integration of AI for automated compliance monitoring and intelligent framework implementation.

Authentic Intelligence: Use of official standards, audit reports, and regulatory guidelines.

MODULE – IV	**08 Hours**

Risk Mitigation and Security Controls - Risk treatment strategies, risk avoidance, mitigation, transfer and acceptance, control selection and implementation, preventive, detective and corrective controls, technical, administrative and physical controls, identity and access management, authentication and authorization, cryptography basics, network and endpoint security, defense-in-depth, zero trust architecture, incident response lifecycle, digital forensics basics, business continuity planning, disaster recovery planning, resilience engineering.

……

Application: Application of security controls, incident response, and business continuity planning in real-world environments.

AI Integration: AI-enabled intrusion detection systems, automated incident response, and adaptive security mechanisms.

Authentic Intelligence: Application of real-time attack signatures, logs, and threat feeds.

MODULE – V	**06 Hours**

Governance, Compliance and Emerging Risks - Cybersecurity governance models, organizational policies, risk governance structure, compliance frameworks, GDPR, HIPAA, PCI-DSS, cyber laws and ethics, audit and assurance, third-party and vendor risk management, supply chain security, cloud security and shared responsibility model, DevSecOps risks, artificial intelligence risks, IoT risks, blockchain risks, ransomware, advanced persistent threats, cyber insurance, privacy and data protection.

……

Application: Application of governance, compliance, and risk management strategies in organizational contexts.

AI Integration: AI-based governance, compliance automation, and risk prediction in emerging technologies.

Authentic Intelligence: Use of regulatory intelligence, cyber laws, and compliance standards for decision-making.

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Explain the concepts, theories, and factors influencing criminal behaviour and behavioural intelligence.	L2
2	Apply psychological and behavioural analysis techniques in criminal investigation and offender assessment.	L3
3	Analyze criminal profiling methods, crime patterns, cyber behaviour, and social media content in investigative contexts.	L4
4	Evaluate behavioural intelligence techniques for crime prevention, threat assessment, and security applications.	L4
5	Assess the role of AI-assisted behavioural analytics and ethical practices in modern criminal psychology and security systems	L

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	1	2	3	4	5	6	7	8	9	10	11	PSO1	PSO2
CO1	3	2	1	-	-	-	2	-	-	-	1	2	1

CO2	3	3	2	2	2	-	2	-	-	-	1	3	2
CO3	3	3	3	2	3	-	2	-	-	-	1	3	3
CO4	2	3	2	2	3	-	3	-	-	-	1	3	2
CO5	2	2	3	2	3	-	3	-	-	-	2	3	3

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Cynthia Brumfield, *Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework*, Wiley, 2021.
2. Douglas W. Hubbard and Richard Seiersen, *How to Measure Anything in Cybersecurity Risk*, Wiley, 2016.

REFERENCE BOOKS:

1. Bruce Schneier, *Liars and Outliers: Enabling the Trust that Society Needs to Thrive*.
2. Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*.
3. Evan Gilman and Doug Barth, *Zero Trust Networks: Building Secure Systems in Untrusted Networks*.
4. *Cybersecurity Risk Management: An Enterprise Risk Management Approach*, Nova Science Publishers, 2022.

AI for IoT & IIoT SECURITY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VI

Course Code	**:**		**Credits**	**:**	03
Hours / Week	**:**	03	**Total Hours**	**:**	45
L–T–P–J	**:**	3–0–0–0	**CIE+SEE**	**:**	60+40 Marks
Course Vision:					

To develop the ability to apply artificial intelligence techniques for securing IoT and IIoT systems against modern cyber threats in real-world environments.

Course Objectives:

This course will enable students:

1. To understand IoT and IIoT architectures, components, and security challenges.
2. To learn common cyber threats and vulnerabilities in IoT and industrial systems.
3. To analyze network, device, and data-level attacks in IoT environments.
4. To apply AI/ML techniques for intrusion detection, anomaly detection, and threat prediction.
5. To design secure IoT/IIoT systems using AI-driven security approaches.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. Use lecture methods supported with visual aids to explain IoT architectures and security threats.
2. Demonstrate real-world IoT attacks and defense mechanisms using tools and simulations.
3. Encourage hands-on learning through AI-based intrusion detection and anomaly detection experiments.
4. Integrate case studies of IoT and IIoT security incidents.
5. Introduce AI/ML tools for analyzing IoT data and detecting cyber threats.
6. Promote mini-projects on AI-driven IoT security solutions.

MODULE – I	**09 Hours**

IoT & IIoT Fundamentals and Security Challenges

Topics: IoT architecture, IIoT systems and industrial environments, sensors and communication layers, IoT protocols (MQTT, CoAP, HTTP), threat landscape in IoT and IIoT, attack surfaces (device, network, cloud), security requirements, introduction to data-driven security approaches.

Applications: Smart home devices, wearable systems, industrial sensing systems, environmental monitoring, connected infrastructure.

Authentic Intelligence: Challenges in securing heterogeneous and resource-constrained IoT devices.

MODULE – II	**09 Hours**

Vulnerabilities and Attack Models

Topics: Device-level attacks, network attacks (DoS, spoofing, MITM), industrial threats (SCADA/ICS attacks), malware and botnets (Mirai), data injection attacks, protocol vulnerabilities, analysis of attack patterns using data-driven methods.

Applications: Security analysis of smart devices, protection against botnet attacks, industrial control system security, network intrusion scenarios.

Authentic Intelligence: Limitations of traditional security methods in dynamic IoT systems.

MODULE – III	**09 Hours**

Machine Learning Techniques for IoT Security

Topics: Introduction to machine learning for security, supervised and unsupervised learning, anomaly detection, classification models (KNN, SVM, Decision Trees), feature extraction from IoT data, datasets for IoT intrusion detection. **Applications:** Intrusion detection systems, anomaly detection in sensor networks, predictive threat analysis, intelligent monitoring systems. **Authentic Intelligence:** Challenges in model accuracy, data quality, and deployment.	
MODULE – IV	**09 Hours**
Intrusion Detection and Industrial IoT Security **Topics:** Intrusion Detection Systems (IDS/IPS), deep learning approaches for anomaly detection, edge-based monitoring, industrial systems (SCADA, ICS), predictive monitoring, real-time threat detection and response. **Applications:** Industrial automation security, SCADA/ICS monitoring, predictive maintenance systems, real-time threat detection platforms. **Authentic Intelligence:** Latency, scalability, and reliability issues.	
MODULE – V	**09 Hours**
Secure IoT Systems and Emerging Security Techniques **Topics:** Secure communication, authentication and access control, lightweight cryptography, blockchain for IoT (overview), federated learning, privacy-preserving techniques, case studies in smart and industrial systems. **Applications:** Secure smart systems, privacy-preserving healthcare systems, secure communication in industrial networks, smart city security solutions. **Authentic Intelligence:** Privacy, ethics, and deployment challenges.	

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Describe IoT and IIoT architectures, components, and security challenges.	L2
2	Explain vulnerabilities and attack models in IoT and industrial systems.	L2
3	Analyze network, device, and data-level attacks in IoT environments.	L3

4	Apply machine learning techniques for intrusion detection and anomaly detection in IoT systems.	L3
5	Develop secure IoT/IIoT systems using AI-driven security approaches.	L5

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	3	2	1	-	-	-	-	-	-	-	1	2	2
CO2	3	3	2	1	-	-	-	-	-	-	1	2	3
CO3	3	3	2	2	2	-	-	-	1	1	1	2	3
CO4	2	3	3	2	3	1	1	2	2	1	1	3	3
CO5	2	3	3	2	3	2	1	2	2	1	1	3	3

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Fei Hu, Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations, 1st Edition, CRC Press, 2016.
2. Brian Russell and Drew Van Duren, Practical Internet of Things Security, 1st Edition, Packt Publishing, 2016.
3. Brij B. Gupta and Pooja Chaudhary, Internet of Things Security: Principles, Applications, Attacks, and Countermeasures, 1st Edition, CRC Press, 2021.

REFERENCE BOOKS:

1. Smita Sharma et al., Artificial Intelligence and IoT for Cyber Security Solutions in Smart Cities, 1st Edition, Chapman & Hall/CRC, 2025.
2. M. M. Islam et al., IoT Security: Advances in Authentication, 1st Edition, Elsevier, 2025.
3. Stuart Russell and Peter Norvig, Artificial Intelligence: A Modern Approach, 4th Edition, Pearson, 2021.

RECOMMENDED TOOLS

- **Programming Languages:** Python, Embedded C
- **Development Platforms:** ESP32, Arduino, Raspberry Pi

- **IoT Communication Tools:** MQTT Broker (Mosquitto), Node-RED
- **Network Analysis Tools:** Wireshark, Scapy
- **AI/ML Tools:** Python libraries (NumPy, Pandas, Scikit-learn, TensorFlow, PyTorch)
- **Simulation Tools :** Cisco Packet Tracer, NS3
- **Cloud Platforms :** ThingSpeak, AWS IoT Core
- **Development Environments:** Google Colab, Jupyter Notebook
- **Version Control:** Git, GitHub

DISK AND MEMORY FORENSICS

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VI

Course Code	:		**Credits**	:	0
Hours / Week	:		**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision: To develop the ability to investigate, analyze, and reconstruct digital evidence from storage media and volatile memory by integrating forensic methodologies, investigative tools, and responsible handling of digital artifacts in real-world cybersecurity scenarios.

Course Objectives: This course will enable students:

1. To understand the fundamentals of digital forensics, file systems, and disk structures.
2. To acquire, preserve, and analyze disk images using forensic tools and techniques.

3. To perform volatile memory acquisition and analyze memory dumps for forensic evidence.
4. To investigate artifacts in file systems, registries, and operating system structures.
5. To apply anti-forensic detection techniques and present forensic findings in professional reports.

Teaching-Learning Process (General Instructions)

These are sample pedagogical methods where the teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with traditional lecture method, different types of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I : Foundations of Disk Structures	**09 Hours**

Topics:

Physical disk structure: platters, sectors, tracks, and cylinders; Logical vs. physical disk addressing; Partitioning schemes: MBR and GPT; File allocation mechanisms and file systems: FAT12/16/32, NTFS, ext2/3/4; File system metadata and forensic significance; Slack space, unallocated space, and deleted file recovery concepts; Introduction to storage artifact analysis in forensic investigations.

Applications:

Understanding how evidence is structured on storage media; Identifying file system artifacts in cybercrime investigations; Legal and procedural guidelines for forensic investigations; Preservation of evidence for court admissibility.

AI Integration:

Introduction to Python-based forensic scripting for disk analysis.

Authentic Intelligence:

Understanding the legal and ethical boundaries of digital investigations; Risks of evidence contamination and chain of custody violations.

MODULE – II : Disk Acquisition & Imaging Techniques	**09 Hours**

Topics:

Disk Acquisition Fundamentals: Write blockers (hardware and software); Forensic imaging formats: RAW/DD, E01 (Expert Witness), AFF; Bit-by-bit imaging vs. logical acquisition; Hashing for integrity verification: MD5, SHA-1, SHA-256. Imaging Tools and Techniques: FTK Imager, dd/dcfldd, Guymager.

Applications:

Acquiring forensic images in incident response scenarios; Verifying the integrity of acquired evidence; Handling encrypted storage in law enforcement investigations; Creating verified forensic duplicates for analysis without altering originals.

AI Integration:

Automated hash verification workflows using Python; Scripting acquisition pipelines with dcfldd and Python wrappers; Using AI-assisted anomaly detection in imaging metadata; Integrating FTK Imager and Guymager into automated forensic pipelines.

Authentic Intelligence:

Risks of evidence alteration during acquisition; Challenges posed by encryption and anti-forensic countermeasures; Ethical considerations in acquiring data from personal devices.

MODULE – III : File System Forensics & Artifact Analysis	**09 Hours**

Topics:

NTFS Forensics: Master File Table (MFT), $LogFile, $UsnJrnl; Alternate Data Streams (ADS); NTFS timestamps (MACB times) and timeline analysis. Windows Artifact Investigation: Registry forensics: hives, keys, and forensic artifacts (UserAssist, MRU, ShimCache, AmCache); Prefetch files, LNK files, Jump Lists, Shellbags. Linux File System Forensics: ext4 journal analysis; inode examination; Bash history, cron jobs, and log analysis (/var/log/).

Applications:

Reconstructing user activity timelines from Windows artifacts; Identifying recently accessed files, installed programs, and USB device history.

AI Integration:

Python scripting for MFT parsing and timeline generation; AI-assisted correlation of artifacts across multiple evidence sources.

Authentic Intelligence:

Privacy implications of forensic access to user activity data. Limitations of automated artifact correlation tools. Validating forensic findings through corroboration of multiple artifact sources.

MODULE – IV : Memory Forensics & Volatile Data Analysis	**09 Hours**

Topics:

Memory acquisition tools: WinPmem, DumpIt, LiME; Memory acquisition from live systems and virtual machines; Memory preservation and forensic integrity. Memory Analysis with Volatility Framework: Introduction to Volatility; Process analysis using pslist, pstree, cmdline, dlllist; Detection of hidden and suspicious processes; Network and handle analysis; DLL and injected code analysis; Malware artifact extraction from memory dumps. Advanced Malware Analysis: DLL injection detection; Process hollowing analysis; Fileless malware indicators; In-memory attack detection; Use of Volatility malfind plugin; Suspicious memory region identification; YARA rule writing for memory forensics; Signature-based malware detection; Correlation of memory artifacts for incident response and threat investigation.

Applications:

Extracting running process information and detecting malware in memory.

AI Integration:

Automated Volatility plugin pipelines using Python scripting; AI-assisted malware classification from memory artifacts; Using YARA rules integrated with Volatility for pattern matching.

Authentic Intelligence:

Risks of false positives in memory-based malware detection; Privacy implications of full memory acquisition (passwords, personal data exposure).

MODULE – V : Anti-Forensics, Reporting & Case Management	**09 Hours**

Topics:

Anti-Forensics Techniques and Detection: Data hiding: steganography, ADS, slack space abuse; File wiping and secure deletion tools: BleachBit, Eraser, Cipher; Timestamp manipulation and metadata scrubbing; Encryption and obfuscation in malware. Forensic Reporting: Structure of a forensic investigation report; Chain of custody documentation.

Applications:

Producing court-admissible forensic reports; Managing multi-source evidence in complex investigations.

AI Integration:

AI-driven detection of steganographic content in files; Automated report generation using forensic case management tools.

Authentic Intelligence:

Risk of bias in AI-assisted forensic conclusions used in legal proceedings; Accuracy and completeness requirements for court-admissible evidence.

Course Outcomes		
Course Outcomes (COs)	**Description**	**Bloom's Taxonomy Level**
At the end of the course the student will be able to:		
1	Identify and explain the fundamentals of digital forensics, disk structures, file systems, and legal frameworks governing forensic investigations.	**L2**
2	Apply disk acquisition techniques using write blockers and forensic imaging tools to acquire and verify evidence from various storage media.	**L3**
3	Analyze Windows and Linux file system artifacts—including registry entries, prefetch files, NTFS metadata, and logs—to reconstruct user activity timelines.	**L4**
4	Acquire and analyze volatile memory using forensic tools to detect running malware, network artifacts, and code injection techniques.	**L4**

5	Evaluate anti-forensic techniques, produce professional forensic investigation reports, and apply emerging forensic methodologies in cloud and containerized environments.	**L5**

Table: Mapping Levels of COs to POs / PSOs

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	2	2	1	-	-	-	-	-	-	-	1	2	2
CO2	2	2	1	-	1	-	-	-	-	-	1	2	2
CO3	3	2	2	1	1	2	1	-	2	1	1	2	2
CO4	3	2	1	1	1	2	1	-	2	1	1	2	2
CO5	3	3	2	1	1	2	1	-	2	1	1	2	2

3: Substantial (High) 2: Moderate (Medium) 1: Poor (Low)

TEXT BOOKS:

1. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory – Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters, Wiley, 1st Edition, 2014.
2. File System Forensic Analysis – Brian Carrier, Addison-Wesley, 1st Edition, 2005.

REFERENCE BOOKS:

1. Incident Response & Computer Forensics – Jason Luttgens, Matthew Pepe, Kevin Mandia, McGraw-Hill, 3rd Edition, 2014.
2. Digital Forensics with Open Source Tools – Cory Altheide & Harlan Carvey, Syngress, 1st Edition, 2011.

RECOMMENDED TOOLS:

Disk Forensics: Autopsy, The Sleuth Kit (TSK), FTK Imager, Guymager, TestDisk/PhotoRec
Memory Forensics: Volatility 3, Rekall, WinPmem, DumpIt, LiME
Timeline & Artifact Analysis: Log2Timeline/Plaso, RegRipper, Shellbags Explorer, PECmd, LECmd
Forensic Platforms: SIFT Workstation, CAINE (Computer Aided Investigative Environment), REMnux
Scripting & Automation: Python (python-evtx, pytsk3, libewf), Jupyter Notebook
AI Assistants: GitHub Copilot, ChatGPT, Claude

OPEN ENDED EXPERIMENTS

S.No	Exercise Title	Aim / Objective	Tools	CO
1	Disk Structure Exploration	Examine MBR/GPT structures and partition tables on a forensic disk image using The Sleuth Kit.	Autopsy / Kali Linux	CO1

2	File System Analysis	Analyze FAT32 and NTFS file systems: identify clusters, inodes, and slack space using Autopsy.	Autopsy / Kali Linux	CO1
3	Forensic Imaging	Acquire a forensic image of a USB drive using FTK Imager and verify integrity with MD5/SHA-256 hashes.	Autopsy / Kali Linux	CO2
4	dd-based Acquisition	Create a bit-stream image using dd/dcfldd and compare with FTK Imager output using hash verification.	Autopsy / Kali Linux	CO2
5	NTFS Artifact Examination	Parse MFT entries and extract MACB timestamps using Python (pytsk3) and Autopsy.	Autopsy / Kali Linux	CO3
6	Windows Registry Forensics	Extract forensic artifacts from registry hives using RegRipper: UserAssist, MRU, ShimCache.	Autopsy / Kali Linux	CO3
7	Memory Acquisition	Acquire a live memory dump using DumpIt/WinPmem and verify dump integrity.	WinPmem / DumpIt	CO4
8	Process & Network Analysis	Use Volatility 3 to enumerate running processes, network connections, and command-line arguments from a memory image.	Volatility 3	CO4
9	Forensic Report Writing	Conduct a complete forensic investigation on a provided disk/memory image and produce a professional investigation report with chain of custody documentation.	Autopsy, Volatility, Plaso	CO5

Secure Coding

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VI

Course Code	:		**Credits**	:	03
Hours / Week	:	03	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

To develop proficient software engineers capable of designing and implementing secure, reliable, and resilient applications by integrating security principles throughout the software development lifecycle with security-first mindset.

Course Objectives:

This course will enable students:

1. **To understand** fundamental concepts of application security, common software vulnerabilities, and the importance of secure coding in modern software development.
2. **To apply** secure coding practices and guidelines to develop robust and error-free programs across different programming environments.
3. **To analyze** various types of security threats such as injection attacks, cross-site scripting, and buffer overflows, and identify their root causes in code.
4. **To evaluate** software systems using vulnerability assessment and testing techniques, including static and dynamic analysis tools.
5. **To design and implement** secure applications by integrating security principles throughout the Secure Software Development Lifecycle (SSDLC).

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with traditional lecture method, different types of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I	**09 Hours**

Fundamentals of Secure Coding

Introduction to secure coding, Software vulnerabilities and threats, Secure Software Development Lifecycle (SSDLC), Principles of secure design (Least Privilege, Defense in Depth, Fail-Safe Defaults), Common weaknesses overview (buffer overflow, injection, XSS, etc.), Introduction to OWASP Top 10

Applications: Software Development & Industry, Cloud & Infrastructure Security, Vulnerability assessment & penetration testing, Secure code review practices.

AI Integration: Vulnerability Detection (AI models detect: Buffer overflows, Injection flaws, Misconfigurations, Tools like AI-based SAST/DAST automate code scanning.

Authentic Intelligence: In Secure Coding Context- Humans define: Secure design principles, Threat models, AI assists: Automated vulnerability scanning, Pattern recognition

NVIDIA DLI Courses (Relevant to this Module):

1. **Fundamentals of Deep Learning** (8 hrs) | Path: https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+C-FX-01+V3

MODULE – II	**09 Hours**

Input Validation and Memory Safety

Input validation techniques (whitelisting vs blacklisting), Secure handling of user inputs, Buffer overflow and memory corruption issues, Format string vulnerabilities, Integer overflow/underflow, Safe string handling in C/C++ and other languages.

Applications: Secure Systems Programming (Preventing buffer overflow, format string, integer overflow in OS-level code, writing safe firmware for embedded systems), Web & Backend Development (Strong input validation (whitelisting) to prevent: SQL Injection, XSS, Command injection).

AI Integration: AI-Based Vulnerability Detection- ML models detect: Buffer overflows, Format string bugs, Unsafe string functions (e.g., gets, strcpy), AI-powered static analysis tools reduce manual effort.

Authentic Intelligence: AI finds hidden vulnerabilities Humans verify and apply secure fixes which reduces: False positives, Missed edge cases

MODULE – III	**09 Hours**

Authentication, Authorization & Cryptography

Secure authentication mechanisms, Password storage (hashing, salting), Session management, Role-Based Access Control (RBAC), Basics of cryptography (encryption, hashing, digital signatures), Common pitfalls in cryptographic implementations

Applications: Web & Application Security (Secure login systems using multi-factor authentication (MFA), Strong password storage (hashing + salting) in web apps, Secure session handling (cookies, tokens, JWT).

AI Integration: AI-Based Authentication (Behavioral biometrics: Typing patterns, Device usage, AI detects suspicious login attempts), Intelligent Fraud Detection (ML models identify: Credential stuffing, Session hijacking).

Authentic Intelligence: AI flags suspicious login → Human verifies, AI detects weak hashing → Developer upgrades implementation

MODULE – IV	**09 Hours**

Secure Coding in Web and Applications

Web vulnerabilities: SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Secure API development, Secure error handling and logging, File handling and secure configuration

Applications: Web vulnerabilities such as SQL Injection, XSS, and CSRF are critical in real-world applications like banking, e-commerce, and cloud platforms, where they help protect databases (e.g., MySQL), web clients, and APIs from unauthorized access and attacks.

AI Integration AI integration enhances these areas by enabling intelligent threat detection, anomaly analysis, automated vulnerability scanning, and real-time protection using tools like Splunk, making security systems more adaptive and proactive.

Authentic Intelligence: Authentic Intelligence combines human expertise with AI to build ethical, explainable, and privacy-aware security solutions, ensuring not only strong protection but also responsible handling of user data and transparent decision-making in cybersecurity systems.

MODULE – V	**09 Hours**

Secure Testing, Tools & Best Practices

Static and dynamic code analysis, Code review techniques, Penetration testing basics, Secure coding standards and guidelines, Use of tools: Static analyzers (SonarQube, Fortify), Vulnerability scanners, Case studies of real-world breaches

Applications: Static and dynamic code analysis, along with structured code review techniques, are widely applied in real-world software development to identify vulnerabilities early and ensure compliance with secure coding standards. Tools like SonarQube and Fortify help automate detection.

AI Integration: Intelligent vulnerability detection, pattern recognition from past exploits, and predictive risk assessment, making security testing faster, scalable, and more accurate..

Authentic Intelligence: Ensure thorough code reviews, ethical security testing, adherence to standards, and transparent decision-making, leading to robust, trustworthy, and secure software systems.

NVIDIA DLI Free Courses (Relevant to this Module):

Exploring Adversarial Machine Learning: (8 Hrs) Path: https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-03+V1

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	**Outline** core concepts of application security, common vulnerabilities, and the Secure Software Development Lifecycle (SSDLC).	L2
2	**Apply** secure coding techniques to handle user inputs safely and prevent memory-related vulnerabilities such as buffer overflows and format string issues.	L3
3	**Make Use of** authentication mechanisms, session management practices, and cryptographic implementations to identify potential security weaknesses.	L3
4	**Analyze** web applications and APIs for vulnerabilities such as SQL injection, XSS, and CSRF using appropriate security testing techniques.	L4
5	Design and develop secure software solutions by incorporating secure coding standards, code review practices, and automated security testing tools.	L3

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	2	2	1	-	-	-	-	-	-	-	-	1	2
CO2	2	2	1	-	-	-	-	-	-	-	-	1	2

CO3	**3**	**2**	**1**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	-	**1**	**2**
CO4	**3**	**2**	**1**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**1**	**2**
CO5	**3**	**2**	**1**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	-	**1**	**2**

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Secure Coding in C and C++ – Robert C. Seacord, Addison Wesley, Second Edition, 2013.
2. The Art of Software Security Assessment – Mark Dowd, John McDonald, Justin Schuh, Addison Wesley Professional, 2006
3. Writing Secure Code – Michael Howard, David LeBlanc, Microsoft Press, Second Edition, 2003.

REFERENCE BOOKS:

1. Web Application Hacker's Handbook – Dafydd Stuttard, Marcus Pinto
2. Secure Coding – John Viega, Gary McGraw

RECOMMENDED TOOLS

- SonarQube – Identifies bugs, code smells, and security issues
- Fortify Static Code Analyzer – Enterprise-grade vulnerability detection
- OWASP ZAP – Open-source web vulnerability scanner
- Burp Suite – Industry-standard web security testing tool
- Kali Linux – Preloaded with security tools

ETHICAL HACKING

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VI

Subject Code	:		**Credits**	:	03
Hours / Week	:	03 Hours	**Total Hours**	:	45
L_T_P_S	:	3-0-0-0			

Course Learning Objectives:

This course will enable students to:

1. To understand and analyze Information security threats & countermeasures
2. To perform security auditing & testing
3. To understand issues relating to ethical hacking
4. To study & employ network defense measures
5. To understand penetration and security testing issues

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts
4. Encourage ***Collaborative*** (Group Learning) Learning in the class
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	09 Hours

ETHICAL HACKING OVERVIEW & PENETRATION TESTING

Understanding the importance of security, Concept of ethical hacking and essential Terminologies Threat, Attack, Vulnerabilities, Target of Evaluation, Exploit. Phases involved in hacking. Penetration Test – Vulnerability Assessments versus Penetration Test – Pre-Engagement – Rules of Engagement - Penetration Testing Methodologies – OSSTMM – NIST – OWASP – Categories of Penetration Test – Types of Penetration Tests – Vulnerability Assessment Summary -Reports.

UNIT_II	09 Hours

FOOTPRINTING & PORT SCANNING

Foot printing - Introduction to foot printing, Understanding the information gathering methodology of the hackers, Tools used for the reconnaissance phase. Port Scanning - Introduction, using port scanning tools, ping sweeps, Scripting Enumeration-Introduction, Enumerating windows OS & Linux OS.

UNIT_III	09 Hours
SYSTEM HACKING8 cracking, Keystroke Loggers, Understanding Sniffers, Comprehending Active and Passive Sniffing, ARP Spoofing and Redirection, DNS and IP Sniffing, HTTPS Sniffing	
UNIT_IV	09 Hours
HACKING WEB SERVICES & SESSION HIJACKING Web application vulnerabilities, application coding errors, SQL injection into Back-end Databases, cross-site scripting, cross-site request forging, authentication bypass, web services and related flaws, protective http headers Understanding Session Hijacking, Phases involved in Session Hijacking, Types of Session Hijacking, Session Hijacking Tools.	
UNIT_V	09 Hours
HACKING WIRELESS NETWORKS Introduction to 802.11, Role of WEP, Cracking WEP Keys, Sniffing Traffic, Wireless Scanners, WLAN Sniffers, Hacking Tools, Securing Wireless Networks. DOS attacks, WLAN	

Course Outcomes:

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

1. **Outline** the influence of security, penetration testing and vulnerability assessment on ethical hacking.
2. **Make use of** port scanning tools like Nmap, OpenVAS and Nessus and ping sweeps such as Hping and Fping to identify open ports and ip addresses of an active host.
3. **Utilize** brute force, key logger, sniffing and spoofing techniques to assess the computational security of a system.
4. **Summarize** sql injection, cross-site scripting and session hijacking techniques to secure e commerce-based web services.
5. **Perceive** network packets of WLAN using modern tools like WLAN Scanners and WLAN Sniffers

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)												PSOs	
CO1												2		
CO2	3	3	2	2	3		2	3				2	2	3
CO3	3	3	2	2	3		2	3				2	2	2
CO4	3		2	1		2		3	2				2	2	2	
CO5	3	2	1	1	3		1	3				2	2	2

3: Substantial (High) 2: Moderate (Medium) 1: Poor (Low)

TEXT BOOKS:

1. Kimberly Graves, "Certified Ethical Hacker", Wiley India Pvt Ltd, 2010
2. Michael T. Simpson, "Hands-on Ethical Hacking & Network Defense", Course Technology, 2010

REFERENCE BOOKS:

1. Rajat Khare, "Network Security and Ethical Hacking", Luniver Press, 2006
2. Ramachandran V, BackTrack 5 Wireless Penetration Testing Beginner's Guide (3rd ed.). Packt Publishing, 2011
3. Thomas Mathew, "Ethical Hacking", OSB publishers, 2003

E-Resources:

1. https://onlinecourses.nptel.ac.in/noc24_cs94/preview
2. https://www.udemy.com/course/complete-ethical-hacking-bootcamp-zero-to-mastery/
3. https://www.coursera.org/projects/metasploit-for-beginners-ethical-penetration-testing
4. https://www.coursera.org/learn/kali-linux

Activity Based Learning (Suggested Activities in Class)

1. vulnerability scanning on a controlled network environment using tools like Nmap, OpenVAS, or Nessus.
2. Organize a Capture the Flag (CTF) competition where students solve various hacking challenges, including web exploitation, cryptography, reverse engineering, and forensics.
3. Create a phishing simulation where students design and execute a phishing campaign within ethical and controlled boundaries.
4. Role-play various social engineering scenarios where students must gather information through techniques like pretexting, baiting, or tailgating.
5. Analyze real-world hacking incidents, discussing the techniques used, the impact, and the countermeasures that could have been implemented.

ADVANCED DATA SCIENCE

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VI

Course Code	**:**		**Credits**	**:**	03
Hours / Week	**:**	3	**Total Hours**	**:**	45
L–T–P–J	**:**	3–0–0–0	**CIE+SEE**	**:**	60+40 Marks

Course Vision:

To develop in students a rigorous and comprehensive understanding of advanced data science methodologies — spanning statistical analysis, advanced machine learning, deep learning, big data engineering, and responsible AI practices — enabling them to independently formulate data-driven solutions for complex, real-world problems across domains such as healthcare, finance, industry, and governance, while upholding ethical standards and societal responsibilities expected of data professionals.

Course Objectives:

This course will enable students:

1. Develop proficiency in the Python data science ecosystem (NumPy, Pandas, Matplotlib, Seaborn, Scikit-learn) for advanced data wrangling, feature engineering, and pipeline construction.
2. Apply exploratory data analysis (EDA) techniques and inferential statistics to derive meaningful insights and validate data assumptions rigorously.
3. Design, train, evaluate, and optimize advanced machine learning models including ensemble methods, SVMs, and probabilistic models using best practices of model selection and hyperparameter tuning.
4. Build and fine-tune deep learning models for structured, image, and sequential data using TensorFlow/Keras, including transfer learning and attention mechanisms.
5. Understand big data processing frameworks, deploy models using MLOps principles, and apply responsible AI practices including fairness, interpretability, and bias mitigation.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with traditional lecture method, different types of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I	**09 Hours**

Advanced Data Engineering & Feature Pipelines

Topics: Advanced Data Wrangling Pipelines, Automated Data Validation, Data Versioning Concepts, Advanced Feature Engineering Strategies, Temporal and Sequential Feature Construction, Feature Stores and Reusable Pipelines, Handling High-Dimensional Data, Advanced Scikit-learn Pipelines and ColumnTransformer, Automated Feature Engineering Concepts (Featuretools, TPOT), Data Leakage and Pipeline Integrity, Data-Centric AI Concepts

Applications: Healthcare data preprocessing for disease prediction systems, Financial time-series feature engineering for stock forecasting

AI Integration: Automated Feature Engineering using AutoML tools (Featuretools, TPOT)

Authentic Intelligence: Recognizing imputation as an assumption — not ground truth; communicating uncertainty in cleaned data

MODULE – II	**09 Hours**

Advanced Statistics & Exploratory Analytics

Topics: Inferential Statistics for Decision Making, Hypothesis Testing in Data Science, Confidence Intervals and Sampling Theory, Probability Distributions in Real Data, Correlation vs Causation, Regression Diagnostics, Multicollinearity Analysis, Statistical Validation of Models, Advanced EDA using Seaborn and Interactive Visualization Tools, Automated EDA Systems (ydata-profiling, SweetViz, D-Tale), Statistical Thinking for AI Systems

Applications: A/B testing for product feature validation in tech companies, Clinical trial data analysis in pharmaceutical research

AI Integration: AI-powered EDA automation tools (Pandas Profiling / ydata-profiling, SweetViz, D-Tale)

Authentic Intelligence: Correlation is not causation — rigorous framing of statistical findings

MODULE – III	**09 Hours**

Advanced Machine Learning & Explainable AI

Topics: Ensemble Learning (Random Forest, Gradient Boosting, XGBoost basics, Voting and Stacking), Support Vector Machines, Probabilistic Learning Models, Advanced Clustering Techniques (DBSCAN, Hierarchical Clustering), Imbalanced Data Handling, Cross-Validation Strategies, Hyperparameter Optimization (Grid Search, Random Search, Bayesian Optimization Concepts), Model Explainability (SHAP, LIME), Bias-Variance Tradeoff, Error Analysis and Model Reliability

Applications: Credit risk scoring and loan default prediction in banking, Medical diagnosis (cancer detection) using ensemble classifiers

AI Integration: AutoML frameworks for automated model selection (Auto-sklearn, H2O AutoML, Google AutoML)

Intelligent rate limiting and anomaly detection using AI middleware

Authentic Intelligence: Responsibility to communicate model uncertainty alongside predictions to decision-makers

MODULE – IV	09 Hours

Applied Generative AI & Intelligent AI Systems

Topics: Introduction to Foundation Models and Generative AI, Practical Use of Pretrained AI Models, Hugging Face Transformers Pipeline API, Zero-shot Classification and Named Entity Recognition, Prompt Engineering Fundamentals for Data Applications, Retrieval-Augmented Generation (RAG) Concepts, Vector Databases and Semantic Search Concepts, AI-Powered Text Analytics and Document Intelligence, AI Model Generalization and Robustness Challenges, Deepfake Detection Fundamentals, AI Hallucination, Reliability and Trustworthiness, Ethical Risks of Generative AI Systems

Applications: Medical image classification (X-ray, MRI analysis) using CNNs and transfer learning, Sentiment analysis and opinion mining using LSTM and BERT

AI Integration: Hugging Face Transformers pipeline API for zero-shot classification and NER without training

Authentic Intelligence: Deepfake risks: societal consequences of generative model misuse and detection responsibility

MODULE – V	09 Hours

Big Data Analytics, MLOps & Responsible AI Systems

Topics: Big Data Fundamentals and 5Vs, Apache Spark and PySpark Essentials, Distributed Data Processing Concepts, MLflow and Experiment Tracking, Model Deployment using FastAPI/Flask, CI/CD for Machine Learning, Containerization Concepts, Model Monitoring and Drift Detection, Responsible AI Principles, Bias and Fairness in AI Systems, Explainability and Governance, Data Privacy Fundamentals (k-anonymity, differential privacy), Scalable AI Infrastructure Concepts

Applications: Large-scale log analysis and anomaly detection at petabyte scale, Real-time recommendation systems deployed via REST microservices

AI Integration: Evidently AI and WhyLabs for automated ML monitoring and drift detection

Authentic Intelligence: Personal accountability of data scientists for downstream societal harm of deployed models

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Construct end-to-end data science pipelines using Pandas, NumPy, and Scikit-learn, implementing feature engineering, dimensionality reduction, and data preprocessing for real-world datasets.	L2
2	Perform rigorous exploratory data analysis using statistical methods (hypothesis testing, correlation analysis, ANOVA) and advanced visualizations to extract actionable insights from complex datasets.	L3
3	Design, train, and optimize advanced machine learning models (ensemble methods, SVMs, Bayesian classifiers) using cross-validation, hyperparameter tuning, and model explainability techniques (SHAP, LIME).	L6
4	Build and fine-tune deep neural networks including CNNs, RNNs/LSTMs, and Transformer-based models using TensorFlow/Keras, applying transfer learning for domain-specific tasks.	L5
5	Evaluate ML models for bias and fairness, deploy models using MLOps tools (MLflow, FastAPI), and process large-scale datasets using Apache Spark fundamentals.	L5

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	**3**	**2**	**3**	**2**	3	-	-	**1**	**2**	**1**	-	**3**	**3**
CO2	**2**	**3**	3	**3**	2	**1**	-	**2**	**2**	-	-	**2**	**3**
CO3	**3**	3	**3**	**3**	3	**2**	-	**2**	**2**	**1**	**2**	**3**	**3**
CO4	**2**	**2**	**3**	**2**	3	-	-	**1**	**2**	-	**2**	**3**	**2**
CO5	**2**	**2**	**3**	**3**	**3**	**3**	**2**	**2**	**3**	**1**	**2**	**2**	**2**

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Aurélien Géron, Hands-On Machine Learning with Scikit-Learn, Keras and TensorFlow, O'Reilly Media, 3rd Edition, 2022.
2. Wes McKinney, Python for Data Analysis: Data Wrangling with pandas, NumPy, and Jupyter, O'Reilly Media, 3rd Edition, 2022.
3. Practical Statistics for Data Scientists Peter Bruce, Andrew Bruce, Peter Gedeck, O'Reilly, 2nd Edition, 2020
4. Designing Machine Learning Systems Chip Huyen, O'Reilly, 2022
5. Hands-On Large Language Models Jay Alammar & Maarten Grootendorst, O'Reilly, 2024

REFERENCE BOOKS:

1. Trevor Hastie, Robert Tibshirani & Jerome Friedman, The Elements of Statistical Learning: Data Mining, Inference, and Prediction, Springer, 2nd Edition, 2009.
2. Christopher M. Bishop, Pattern Recognition and Machine Learning, Springer, 2006.

RECOMMENDED TOOLS

- Development Environment: Jupyter Lab / Jupyter Notebook / Google Colab (cloud, free GPU) / VS Code with Jupyter extension
- Version Control: Git 2.40+ | GitHub / GitLab | GitHub Desktop (beginners) | GitKraken (visual Git history)
- Machine Learning: Scikit-learn 1.3+, XGBoost, LightGBM, CatBoost, Optuna, SHAP, LIME
- AI Assistants: GitHub Copilot, ChatGPT, Claude

NETWORK SECURITY ESSENTIALS

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VI

Course Code	:		**Credits**	:	03
Hours / Week	:	03	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

To create awareness and understanding of network security principles and enable students to identify, analyze, and apply security mechanisms to protect digital communication systems.

Course Objectives:

This course will enable students:

1. Understand fundamental concepts of network security and common threats.
2. Identify different types of network attacks and vulnerabilities.
3. Explain basic security mechanisms used in networks.
4. Apply secure communication practices and authentication methods.
5. Develop awareness of cyber threats and preventive measures.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with presentation-based teaching may be adopted to explain fundamental concepts of network security.
2. **Interactive Teaching**: incorporating brainstorming, discussions, group work, and Q&A sessions on real-world cyber threats and attacks.
3. **Showing video/animation films** to demonstrate working of network protocols, encryption techniques, and security mechanisms.
4. **Encourage Collaborative (Group Learning) learning** in the class through case studies and problem-solving activities.
5. To develop critical thinking, **asking higher order thinking questions** in the form of quizzes and scenario-based problems.
6. **Demonstrating multiple approaches** to solving security problems and encouraging students to propose their own solutions.

MODULE – I: Network Security Fundamentals and Threats	**09 Hours**

Overview of computer networks, network topologies, categories of networks, Internet basics, OSI and TCP/IP models, comparison of OSI and TCP/IP models. Security concepts: CIA Triad, security services, mechanisms, and attacks, OSI Security Architecture, Network Security Model. Common threats and attacks: malware, phishing, social engineering, and basic network vulnerabilities.

Applications: Secure Internet usage, Protection of personal and organizational data, Safe online communication

AI Integration: AI-based threat detection systems, Intelligent monitoring of network traffic

Authentic Intelligence: Awareness of cyber risks in digital environments, Responsible use of digital resources

MODULE – II: Authentication and Classical Cryptographic Techniques	**09 Hours**

Network attacks: DoS/DDoS, Man-in-the-Middle attack, spoofing, password attacks, malware attacks. Authentication mechanisms: passwords, OTP, multi-factor authentication, PKI, digital certificates. Classical encryption techniques: symmetric cipher model, substitution techniques, transposition techniques, steganography. Electronic mail security: email threats, PGP, S/MIME.

Applications: Secure communication systems, User authentication and access control, Secure email communication

AI Integration: AI-based intrusion detection, Pattern recognition in cyber-attacks

Authentic Intelligence: Ethical handling of security threats, Importance of proactive security practices

MODULE – III: Network Security Mechanisms and Encryption	**09 Hours**

Introduction to encryption techniques: symmetric and asymmetric encryption concepts. Firewalls: types, characteristics, and functions. Intrusion Detection and Prevention Systems (IDS/IPS). Antivirus and anti-malware tools. Virtual Private Networks (VPN): concepts, types, and applications.

Applications: Enterprise network protection, Secure remote access, Malware prevention and monitoring

AI Integration: AI-driven firewall and IDS systems, Automated threat detection and monitoring

Authentic Intelligence: Responsible configuration of security tools, Avoiding misuse of security mechanisms

MODULE – IV: Secure Communication Protocols and Web Security	**09 Hours**

Secure communication concepts, HTTPS, SSL/TLS, SSH. Wireless network security: WiFi security, WPA concepts. DNS security basics. Authentication techniques and secure communication protocols. Web security considerations and secure online transactions.

Applications: Secure web browsing, Online banking and e-commerce security, Organizational communication security

AI Integration: AI-enabled authentication systems, AI-assisted secure communication analysis

Authentic Intelligence: Safe handling of sensitive communication, Awareness of secure authentication practices

MODULE – V: System Security, Cyber Defense, and Security Applications	**09 Hours**
System security concepts, intrusion detection, malware analysis, password management. Firewalls and protection mechanisms in real-world systems. Cyber security best practices, safe browsing, data privacy, and cyber hygiene. Case studies of cyber-attacks and data breaches. Introduction to ethical hacking and security testing concepts. Role of AI in cybersecurity monitoring, anomaly detection, and cyber defense systems. **Applications:** Organizational cyber defense strategies, Security monitoring and incident response, Real-world cybersecurity practices **AI Integration:** AI-based user behavior analysis, Intelligent threat monitoring systems **Authentic Intelligence:** Responsible digital behavior, Ethical and secure use of technology	

Course Outcome

Course Outcomes (COs)	**Description**	**Bloom's Taxonomy Level**
At the end of the course the student will be able to:		
1	Explain networking fundamentals, Internet architecture, security services, mechanisms, security models, and common network threats and attacks	L2
2	Apply authentication methods, classical cryptographic techniques, and secure email mechanisms such as PGP and S/MIME for secure communication	L3
3	Apply network security mechanisms including encryption techniques, firewalls, IDS/IPS, antivirus tools, and VPN for protecting network systems	L3
4	Analyze secure communication protocols and web security mechanisms such as SSL/TLS, HTTPS, SSH, wireless security, and DNS security	L4
5	Evaluate system security mechanisms, cyber defense strategies, malware analysis, ethical hacking concepts, and AI-based network security monitoring techniques	L5

Mapping Levels of COs to POs / PSOs

				Table: Mapping Levels of COs to POs / PSOs									
COs				Program Outcomes (POs)								PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	3	2	-	-	-	-	-	-	-	-	1	2	2
CO2	3	3	2	1	2	-	-	-	-	-	1	3	2
CO3	3	2	2	1	2	-	-	-	-	-	1	3	3
CO4	3	3	2	2	2	-	-	-	-	-	1	3	3
CO5	3	3	3	2	2	1	1	-	-	-	2	3	3

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Data Communications and Networking, Fifth Edition, McGraw-Hill Education, 2013.
2. Network Security Essentials: Applications and Standards, Sixth Edition, Pearson Education, 2017.

REFERENCE BOOKS:

3. Cryptography and Network Security: Principles and Practice, Seventh Edition, Pearson Education, 2017.
4. Network Security: Private Communication in a Public World, Second Edition, Prentice Hall, 2002.
5. Cryptography and Network Security, Third Edition, McGraw-Hill Education, 2015.
6. Cryptography and Network Security, Fourth Edition, McGraw-Hill Education, 2019.

RECOMMENDED TOOLS

- Wireshark (Packet Analysis)
- OpenSSL (Encryption & Certificate Management)
- VirtualBox / VMware (Network Simulation)
- Kali Linux Tools (Security Testing)
- Snort (Intrusion Detection System)

CYBER SECURITY ESSENTIALS

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VI

Course Code	:		**Credits**	:	03
Hours / Week	:	03	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

To develop foundational and applied competencies in cybersecurity, enabling learners to understand, analyse, and mitigate cyber threats using modern tools, ethical practices, and intelligent technologies.

Course Objectives:

The course aims to enable students to:

1. To introduce core principles of cybersecurity and threat landscape
2. To develop skills in securing systems, networks, and applications
3. To provide exposure to cyber laws, risk management, and ethical practices
4. To integrate AI-driven security approaches and authentic intelligence analysis
5. To prepare students for real-world cybersecurity problem-solving

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with traditional lecture method, different types of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I: Fundamentals of Cyber Security	**09 Hours**

CIA Triad (Confidentiality, Integrity, Availability), Cyber Security Terminology and Concepts, Types of Cyber Threats: Malware, Phishing, Social Engineering, Insider Threats, Advanced Persistent Threats (APTs), Attack Vectors and Attack Surfaces, Cyber Kill Chain Model.

Applications: Enterprise Security Awareness, Threat Modelling in Organizations, Incident Response Planning AI Integration: AI-based phishing detection systems, Malware classification using Machine Learning models Authentic Intelligence: Human judgment in identifying social engineering attacks, Analyst-driven interpretation of cyber threats	
MODULE – II: Network Security and Defence Mechanisms	**09 Hours**
Network Security Architecture and Security Concepts, OSI & TCP/IP Security Issues, Common Network Attacks: DoS/DDoS, Man-in-the-Middle (MITM), Packet Sniffing and Spoofing. Firewalls: Packet Filtering, Stateful and Proxy Firewalls, Intrusion Detection and Prevention Systems (IDS/IPS), Virtual Private Networks (VPNs), Wireless Network Security (WEP, WPA, WPA2, WPA3). **Applications:** Secure Network Design, Firewall Configuration, Traffic Monitoring. **AI Integration:** AI-based intrusion detection and anomaly detection. **Authentic Intelligence:** Human validation of anomaly detection systems.	
MODULE – III: Cryptography and Data Protection	**09 Hours**
Introduction to Cryptography, Symmetric Encryption (AES, DES), Asymmetric Encryption (RSA), Hash Functions (SHA Family, MD5 Limitations), Digital Signatures and Digital Certificates. Public Key Infrastructure (PKI), Key Management and Distribution, Basics of Blockchain Security. **Applications:** Secure Communication, E-Commerce Security, Data Integrity Verification. **AI Integration:** Automated certificate management and blockchain analytics. **Authentic Intelligence:** Ethical use of cryptographic systems.	
MODULE – IV: System Security and Risk Management	**09 Hours**
Operating System Security, Access Control Models (DAC, MAC, RBAC), Vulnerability Assessment and Penetration Testing (VAPT), Malware Analysis Basics. Risk Management: Risk Identification, Assessment and Mitigation, Security Policies and Governance, Backup and Disaster Recovery, Security Auditing. **Applications:** Security Audits, Risk Assessment, Incident Handling. **AI Integration:** AI-based vulnerability scanners and automated penetration testing. **Authentic Intelligence:** Human prioritization of risks and interpretation of scan results.	
MODULE – V: Cyber Laws, Emerging Security Technologies, and Ethical Practices	**09 Hours**
Cyber Ethics and Professional Responsibility, Information Technology Act 2000, Data Protection and Privacy Laws, Digital Forensics Basics.Emerging Security Technologies: Cloud Security, IoT Security, Zero Trust Architecture, AI in Cybersecurity. Cyber Ethics and Professional Responsibility, Information	

Technology Act 2000, Data Protection and Privacy Laws, Digital Forensics Basics. Emerging Security Technologies: Cloud Security, IoT Security, Zero Trust Architecture, AI in Cybersecurity.

Applications: Legal Compliance, Digital Investigations, Secure Cloud Deployment.

AI Integration: Threat intelligence platforms and forensic automation tools.

Authentic Intelligence: Ethical reasoning in cyber investigations and responsible AI usage.

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Explain cybersecurity fundamentals, cyber threats, attack vectors, and security principles for protecting information systems	L2
2	Apply network security mechanisms including firewalls, IDS/IPS, VPNs, wireless security techniques, and defense strategies to protect communication systems	L3
3	Apply cryptographic techniques, digital signatures, certificates, PKI, and key management mechanisms for secure data communication and protection	L3
4	Analyze system vulnerabilities, access control models, malware behavior, and risk management techniques for securing computing environments	L4
5	Evaluate cyber laws, ethical practices, digital forensic methods, and emerging security technologies for addressing modern cybersecurity challenges	L5

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	3	2	-	-	-	-	1	-	-	-	1	2	2
CO2	3	3	2	1	3	-	1	-	-	-	1	3	3
CO3	3	2	2	1	2	-	1	-	-	-	1	3	3

CO4	3	3	2	2	2	1	1	-	-	-	2	3	3
CO5	2	3	2	2	2	2	3	-	-	-	2	2	3

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Cybersecurity Essentials Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short, *Cybersecurity Essentials*, First Edition, Cisco Press (Pearson Education), 2018, ISBN: 978-1587134388.
2. Computer Security: Principles and Practice William Stallings, Lawrie Brown, *Computer Security: Principles and Practice*, Fourth Edition, Pearson Education, 2018, ISBN: 978-0134794105.

REFERENCE BOOKS:

1. Cryptography and Network Security: Principles and Practice William Stallings, *Cryptography and Network Security: Principles and Practice*, Seventh Edition, Pearson Education, 2017, ISBN: 978-0134444284.
2. The Web Application Hacker's Handbook Dafydd Stuttard, Marcus Pinto, *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*, Second Edition, Wiley Publishing, 2011, ISBN: 978-1118026472.
3. Hacking: The Art of Exploitation Jon Erickson, *Hacking: The Art of Exploitation*, Second Edition, No Starch Press, 2008, ISBN: 978-1593271442.
4. Cyber Security Nina Godbole, Sunit Belapure, *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*, First Edition, Wiley India, 2011, ISBN: 978-8126521791.
5. Network Security Essentials: Applications and Standards William Stallings, *Network Security Essentials: Applications and Standards*, Sixth Edition, Pearson Education, 2017, ISBN: 978-0134527338.

RECOMMENDED TOOLS

- **Wireshark** – Network traffic analysis
- **Nmap** – Network scanning and security analysis
- **Metasploit Framework** – Vulnerability assessment and penetration testing
- **OpenSSL** – Encryption and certificate management
- **Python** – Security automation and AI-based analysis
- **VirtualBox / VMware** – Security and network simulation

CRYPTOGRAPHY AND NETWORK SECURITY [As per Choice Based Credit System (CBCS) scheme] SEMESTER - V					
Course Code	:		**Credits**	:	03
Hours / Week	:	03	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

To develop strong theoretical and practical knowledge in cryptography and network security, enabling students to design and implement secure communication systems.

Course Objectives:

This course will enable students to:

- To understand classical and modern cryptographic techniques.
- To apply number theory and encryption algorithms in secure systems.
- To implement symmetric and asymmetric cryptographic techniques.
- To analyze authentication and digital signature mechanisms.
- To evaluate network security applications and real-world threats.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

- **Lecture method** along with presentation-based teaching to explain cryptographic concepts.

○ **Interactive Teaching:** brainstorming, discussions, and case studies on real-world security scenarios. ○ **Showing video/animation films** to demonstrate encryption, hashing, and secure communication. ○ **Encourage Collaborative (Group Learning) learning** through mini-projects and problem-solving. ○ To **develop critical thinking, asking higher order thinking questions** through quizzes and case-based analysis. **Demonstrating multiple approaches** to solve security problems and encouraging innovative solutions.	
MODULE – I	**09 Hours**
Overview: Services, Mechanisms and attacks, OSI Security Architecture, Network Security Model. Classical Encryption Techniques: Symmetric cipher model, Substitution Techniques, Transposition Techniques, Steganography.	
MODULE – II	**10 Hours**
Finite Fields and Number Theory: Groups, Rings, Fields, Modular Arithmetic, Euclid's Algorithm, Finite Fields, Polynomial Arithmetic. Prime Numbers, Fermat's and Euler's Theorem, Testing for Primality, Chinese Remainder Theorem, Discrete Logarithms. Block Cipher Principles, Data Encryption Standard (DES), Triple DES, Block Cipher Modes of Operation, Advanced Encryption Standard (AES).	
MODULE – III	**10 Hours**
Public Key Cryptography: Principles of public key cryptosystems, RSA algorithm, ElGamal cryptosystem, Elliptic Curve Cryptography (ECC). Key Agreement: Diffie-Hellman key exchange, Key management and distribution. Hash Functions: SHA, MAC, Authentication requirements, Authentication functions, Security of MAC, HMAC, CMAC.	
MODULE – IV	**08 Hours**
Digital Signatures: ElGamal, Schnorr, DSS. Authentication Applications: One-way authentication, Mutual authentication. Kerberos, X.509 Authentication Services.	
MODULE – V	**08 Hours**
Electronic Mail Security: PGP, S/MIME. IP Security, Web Security, System Security. Intruders, Malicious Software (viruses), Firewalls.	

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Explain security services, mechanisms, security attacks, OSI security architecture, network security model, and classical encryption techniques including substitution, transposition, and steganography	L2
2	Apply number theory concepts including modular arithmetic, Euclid's algorithm, finite fields, prime number theorems, and discrete logarithms to analyze and implement symmetric key cryptographic algorithms such as DES, Triple DES, AES, and block cipher modes	L3
3	Apply principles of public key cryptography including RSA, ElGamal, ECC, Diffie-Hellman key exchange, key management techniques, and cryptographic hash functions such as SHA, MAC, HMAC, and CMAC	L3

	for secure communication	
4	Analyze digital signature algorithms (ElGamal, Schnorr, DSS), authentication mechanisms including one-way and mutual authentication, and security services such as Kerberos and X.509 authentication frameworks	L4
5	Evaluate network and system security mechanisms including PGP, S/MIME, IP security, web security, intrusion techniques, malware threats, and firewall protection strategies	L5

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
	Engineering knowledge	Problem analysis	Design/Development of Solutions	Conduct investigations of complex problems	tool usage	The engineer and society	Ethics	team work	Communication	Project management and finance	Life-long learning	Programming & core computing skills	Cybersecurity & data protection skills
CO1	3	2	-	-	-	-	-	-	-	-	1	2	2
CO2	3	3	2	1	2	-	-	-	-	-	1	3	2
CO3	3	2	2	1	2	-	-	-	-	-	1	3	3
CO4	3	3	2	2	2	-	-	-	-	-	1	3	3
CO5	2	3	2	2	2	1	1	-	-	-	2	2	3

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

- William Stallings, Cryptography and Network Security: Principles and Practice, Pearson, 8thEdition, 2019, ISBN: 9780135764039,0135764033..

REFERENCE BOOKS:

7. BehrouzA.Foruzan, Cryptography and Network Security, Tata McGraw Hill 2007.
8. C K Shyamala, N Harini and Dr. T R Padmanabhan: Cryptography and Network Security, Wiley India Pvt.Ltd
9. Cryptography and Network Security: Atul Kahate, Mc Graw Hill, 3rd Edition..

RECOMMENDED TOOLS

6. Programming: Python (Cryptography, hashlib, PyCryptodome), C/C++ (optional) – Jupyter Notebook / VS Code
7. Security Tools: OpenSSL, GnuPG (GPG), Wireshark, Nmap
8. Network Simulation: VirtualBox / VMware, Kali Linux
9. Web Security Tools: Burp Suite (Community), Browser DevTools
10. Monitoring & IDS: Snort (basic), Zeek (optional)
11. AI Assistants: GitHub Copilot, ChatGPT

OPEN ENDDED **XERCISES**

S.No	Exercise Title	Aim / Objective	Tools	Hrs	CO
MODULE I · Exercises 1–3 : Classical Cryptography & Security Basics					**(06 Hours)**
1	Caesar Cipher	Implement Caesar Cipher and perform encryption and decryption	Python	2 h	CO1
2	Transposition Cipher	Implement transposition cipher techniques for secure communication	Python	2 h	CO1
3	Steganography	Hide and extract secret data using image-based steganography	Python	2 h	CO1
MODULE II · Exercises 4–7 : Symmetric Cryptography & Number Theory					**(08 Hours)**
4	Euclid Algorithm	Implement Euclid's algorithm to compute GCD and modular inverse	Python	2 h	CO2
5	Modular Arithmetic	Perform modular exponentiation and inverse operations	Python	2 h	CO2
6	DES/AES Implementation	Demonstrate encryption and decryption using DES/AES	OpenSSL / Python	2 h	CO2
7	Block Cipher Modes	Compare ECB and CBC modes of operation	Python	2 h	CO2
MODULE III ·Exercises 8–10 : Public Key Cryptography					**(06 Hours)**
8	RSA Algorithm	Implement RSA encryption and decryption	Python	2 h	CO3
9	Diffie-Hellman	Simulate secure key exchange between two users	Python	2 h	CO3

S.No	Exercise Title	Aim / Objective	Tools	Hrs	CO
10	Hash Functions	Generate and verify SHA hash and MAC values	Python	2 h	CO3
MODULE IV · Exercises 11-12 : Authentication & Digital Signatures					**(04 Hours)**
11	Digital Signature	Implement digital signature generation and verification	Python	2 h	CO4
12	Certificate Analysis	Analyze X.509 certificates using OpenSSL	OpenSSL	2 h	CO4
MODULE V · Exercises 13–15 : Network & System Security					**(06 Hours)**
13	Secure Email	Demonstrate PGP or S/MIME for secure email communication	GPG / Tool-based	2 h	CO5
14	Packet Analysis	Capture and analyze HTTPS traffic using Wireshark	Wireshark	2 h	CO5
15	Firewall & Network Scan	Configure basic firewall rules and perform scanning using Nmap	Linux / Nmap	2 h	CO5

AI IN QUANTUM CRYPTOGRAPHY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – VII

Course Code	:		**Credits**	:	03
Hours / Week	:	3	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

To develop the ability to understand, design, and analyze secure communication systems using principles of quantum mechanics and cryptography for next-generation cyber security applications.

Course Objectives:

This course will enable students:

1. To summarize the fundamentals of Artificial Intelligence and Quantum Cryptography.
2. To understand the role of AI in quantum communication and cryptographic systems.
3. To apply AI techniques for optimizing quantum key distribution and protocols.
4. To analyze quantum attacks and develop intelligent defense mechanisms.
5. To evaluate performance, security, and scalability of AI-driven quantum cryptographic systems.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. Lecture method along with traditional lecture delivery may be adopted to explain AI and quantum cryptography concepts effectively.
2. Interactive Teaching: incorporating brainstorming, discussions, group work, and AI-based problem-solving tasks.
3. Showing video/animation films to visualize quantum states, neural networks, and secure communication models.
4. Encourage Collaborative (Group Learning) through AI-based cryptographic case studies and simulations.
5. Demonstrations using AI tools and quantum simulators for practical understanding.
6. To develop critical thinking through quizzes and complex problem-solving involving AI and quantum security.

MODULE – I	**09 Hours**

Foundations of AI Quantum Computing

Topics: Basics of Artificial Intelligence, Machine Learning Overview, Quantum Computing Fundamentals, Qubits, Superposition, Entanglement, Classical vs Quantum Cryptography.

Applications: Intelligent secure systems, quantum-enhanced AI models, cryptographic system design.

AI Integration: Implementation of basic ML models using Python, simulation of quantum circuits using Qiskit.

Authentic Intelligence: Challenges in integrating AI with quantum systems, limitations of current quantum hardware, risks in hybrid systems.

NVIDIA DLI Courses (Relevant to this Module):

1. **Accelerating End-to-End Data Science Workflows** (8 hrs) | Path: Data Science Training - Accelerated Data Science Foundations

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-01+V2

2. **Best Practices in Feature Engineering for Tabular Data With GPU Acceleration** (2 hrs) | Path: Accelerated Data Science Foundations

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-06+V1

MODULE – II	**09 Hours**

AI-Driven Quantum Key Distribution (QKD)

Topics: BB84 and E91 Protocols, Quantum Key Distribution, Noise and Error Handling, AI-based Optimization of QKD, Reinforcement Learning for Channel Optimization.

Applications: Secure communication in defense, finance, and critical infrastructures.

AI Integration: Use of machine learning models to optimize key generation rates, error correction, and intrusion detection.

Authentic Intelligence: Limitations due to noise, real-world deployment challenges, reliability of AI-driven optimization.

MODULE – III	**09 Hours**

Quantum Cryptographic Protocols with AI

Topics: Quantum Teleportation, Quantum Digital Signatures, Quantum Authentication, AI-based Protocol Optimization, Intelligent Security Models.

Applications: Identity verification, secure communication networks, smart cryptographic systems.

AI Integration: Modeling Deep learning for anomaly detection, AI-driven protocol simulation and optimization.

Authentic Intelligence: Risks of AI misclassification, scalability challenges, complexity in hybrid protocol design.

NVIDIA DLI Free Courses (Relevant to this Module):

1. **Accelerating Clustering Algorithms to Achieve the Highest Performance** (2 hrs) | Path: Data Science Training – Accelerated Data Science Foundations

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-04+V1

MODULE – IV	**09 Hours**

Post-Quantum Cryptography and AI

Topics: Lattice-based Cryptography, Hash-based Cryptography, Code-based Cryptography, AI-based Cryptanalysis, Performance Optimization using AI.

Applications: Future-proof encryption systems, secure internet protocols, enterprise cybersecurity.

AI Integration: Machine learning for cryptanalysis, optimization of cryptographic algorithms, predictive security modeling.

Authentic Intelligence: Trade-offs between efficiency and security, risks of AI-based attacks, computational overhead.

NVIDIA DLI Courses (Relevant to this Module):

1. **Exploring Adversarial Machine Learning** (8 hrs) | Path: Deep Learning Training – AI Security Engineering & Federated ML

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-03+V1

MODULE – V	**09 Hours**

Quantum Attacks, AI Defense and Security Evaluation

Topics: Shor's Algorithm, Grover's Algorithm, Quantum Attacks on Classical Cryptography, AI-based Threat Detection, Security Evaluation and Risk Analysis.

Applications: Cybersecurity defense systems, intrusion detection, risk assessment in quantum environments.

AI Integration: AI models for anomaly detection, predictive threat analysis, automated security evaluation.

Authentic Intelligence: Ethical concerns, reliability of AI decisions, limitations in real-world quantum attack scenarios.

NVIDIA DLI Free Courses (Relevant to this Module):

1. **Accelerate Data Science Workflows with Zero Code Changes** (1 hr) | Path: Data Science Training – Data Preparation for Model Training

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+T-DS-03+V1

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Recall fundamental concepts of AI and quantum cryptography.	L1
2	Describe AI techniques and quantum cryptographic principles.	L2
3	Apply AI methods to quantum key distribution and protocols.	L3
4	Analyze post-quantum cryptography and AI-based security mechanisms.	L4
5	Evaluate performance and security of AI-driven quantum cryptographic systems.	L5

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	1	1	-	-	-	-	-	-	-	-	1	1	1
CO2	2	2	1	-	-	-	-	-	-	-	1	2	2
CO3	3	2	1	1	1	2	1	-	2	1	1	2	2
CO4	3	2	1	1	1	2	1	-	2	1	1	2	2
CO5	3	2	1	1	1	2	1	-	2	1	1	2	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Quantum Computation and Quantum Information – Michael A. Nielsen & Isaac L. Chuang, Cambridge University Press, 2010.
2. Hands-On Machine Learning with Scikit-Learn, Keras & TensorFlow – Aurélien Géron, O'Reilly Media, 2022.

REFERENCE BOOKS:

1. Post-Quantum Cryptography – Daniel J. Bernstein et al., Springer, 2009
2. Artificial Intelligence: A Modern Approach – Stuart Russell & Peter Norvig, Pearson, 3rd Edition.

RECOMMENDED TOOLS

Programming: Python (NumPy, Pandas, Scikit-learn, Qiskit, Cirq) – Google Colab/ Jupyter Notebook

Quantum Platforms: IBM Quantum Experience, Azure Quantum

AI Tools: TensorFlow, PyTorch

Simulation: Qiskit Aer, Cirq Simulator

Visualization: Matplotlib, Plotly

AI Assistants: GitHub Copilot, ChatGPT, Claude

NETWORK FORENSICS

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VII

Course Code	:		**Credits**	:	03
Hours / Week	:		**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision: To develop the ability to capture, decode, reconstruct, and investigate network traffic and protocol-level artifacts using forensic methodologies, enabling identification of intrusions, data exfiltration, and cyber attacks across wired, wireless, and cloud network environments.

Course Objectives: This course will enable students:

1. To understand network communication models, traffic capture methodologies, and forensic investigation frameworks for network-based evidence.
2. To capture, filter, and analyze network packet data using professional forensic tools for protocol-level investigation.
3. To reconstruct network sessions, identify attack patterns, and trace threat actors from network traffic and log evidence.
4. To investigate wireless network forensics, intrusion detection logs, and firewall artifacts for evidence of unauthorized access.
5. To apply network forensics techniques in cloud, encrypted traffic, and dark web environments, and produce professional investigation reports.

Teaching-Learning Process (General Instructions)

These are sample pedagogical methods where the teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with traditional lecture method, different types of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I : Foundations of Network Forensics & Traffic Capture	**09 Hours**

Topics:

Introduction to Network Forensics: Scope, objectives, and role in incident response; Legal framework for network evidence collection; Network forensics vs. network monitoring; Chain of custody for network artifacts. Network Communication Models: OSI and TCP/IP model review from a forensic perspective; Packet structure and header analysis; Network addressing: IPv4, IPv6, MAC addressing, ARP. Traffic Capture Fundamentals: Packet capture methods: promiscuous mode, port mirroring (SPAN), network taps; Capture file formats: PCAP, PCAPNG; Selective and full packet capture strategies; Introduction to capture tools: tcpdump, Wireshark, tshark.

Applications:

Identifying and preserving network traffic evidence for legal proceedings; Analyzing packet headers to determine communication endpoints and protocols.

AI Integration:

AI-assisted anomaly detection in baseline network traffic.

Authentic Intelligence:

Legal and ethical constraints on capturing network traffic without authorization; Chain of custody requirements for network evidence admissibility.

MODULE – II : Protocol Analysis & Network Traffic Reconstruction	**09 Hours**

Topics:

Deep Packet Inspection and Protocol Forensics: HTTP/HTTPS traffic analysis: request/response reconstruction, URI patterns, user-agent analysis; DNS forensics: query logs, DNS tunneling detection, zone transfer artifacts, email header analysis. TCP Stream Reconstruction: TCP session reassembly and flow analysis; Identifying incomplete sessions and retransmission artifacts; Extracting files and objects from raw packet streams; Application-layer data carving from PCAP files. Network Flow Analysis: NetFlow/IPFIX and sFlow concepts; Flow record forensics: src/dst IP, port, byte counts, duration; Identifying beaconing, port scanning, and lateral movement from flow data.

Applications:

Reconstructing web browsing sessions and downloaded files from captured HTTP traffic; Detecting command-and-control (C2) beaconing from NetFlow records.

AI Integration:

Python scripts for DNS query log analysis and tunneling detection; Integrating Zeek script framework for automated protocol forensics and alert generation.

Authentic Intelligence:

Ethical boundaries of credential recovery from captured authentication sessions; Risks of misclassification in machine learning-based protocol analysis.

MODULE – III : Intrusion Detection & Log Forensics	**09 Hours**

Topics:

Intrusion Detection System (IDS) Log Forensics: Snort and Suricata alert log analysis; Rule-based and anomaly-based detection artifacts; Correlation of IDS alerts with raw packet captures (PCAP); False positive identification and alert triage; Incident response and forensic readiness exercise involving simulated IDS alerts, PCAP correlation, firewall log analysis, structured triage reporting, and containment recommendation development. Firewall and Router Log Analysis: Firewall rule hit analysis; Blocked and allowed traffic pattern analysis; Router syslog forensics including interface statistics, routing changes, and access control hits; NAT log analysis for source IP attribution; Log aggregation using syslog and SIEM integration. Attack Pattern Recognition: Port scanning and reconnaissance signatures including Nmap fingerprinting; Detection of DoS and DDoS traffic patterns such as SYN flood and amplification attacks.

Applications:

Correlating IDS alerts with packet captures to confirm intrusion events; Attributing attacks to source IPs through firewall and NAT log analysis.

AI Integration:

Automated Snort/Suricata log parsing with Python and ELK Stack.

Authentic Intelligence:

Ethical responsibilities when reporting attribution findings in legal proceedings; Accuracy limitations of rule-based IDS in detecting zero-day and polymorphic attacks.

MODULE – IV : Wireless Network Forensics & Encrypted Traffic Analysis	**09 Hours**

Topics:

Wireless Network Forensics: IEEE 802.11 frame structure: management, control, and data frames; Wireless traffic capture: monitor mode, promiscuous mode; WEP, WPA, WPA2, and WPA3 security analysis; De-authentication and disassociation attack artifacts; Rogue access point detection and evil twin forensics; Bluetooth forensics: device pairing artifacts, HCI logs.

Applications:

Capturing and analyzing 802.11 wireless frames to identify unauthorized access and rogue Aps.

AI Integration:

Automated wireless frame analysis using Aircrack-ng suite and Scapy.

Authentic Intelligence:

Ethical challenges of analyzing encrypted communications without lawful interception authority.

MODULE – V : Cloud Network Forensics & Dark Web	**09 Hours**

Topics:

Cloud Network Forensics: Cloud network architectures: VPC, security groups, and flow logs (AWS VPC Flow Logs); Cloud WAF and load balancer access log analysis; Serverless function and API gateway traffic forensics; Cloud storage access log forensics: S3 access logs. Dark Web and Anonymizing Network Forensics: Tor network architecture and exit node traffic identification; I2P and Freenet traffic characterization

Applications:

Collecting and analyzing VPC flow logs to reconstruct attacker lateral movement in cloud environments; Identifying data staging and exfiltration through cloud storage access logs; Detecting Tor exit node usage in enterprise network logs; Producing court-admissible network forensic investigation reports from multi-source evidence.

AI Integration:

Automated VPC flow log ingestion and anomaly detection using Python and AWS Athena; Machine learning-based classification of dark web traffic signatures from gateway logs; Zeek-based detection of Tor and I2P traffic using behavioral heuristics; AI-assisted correlation of cloud API logs with network flow data for incident reconstruction; Automated report generation from Xplico and NetworkMiner case exports.

Authentic Intelligence:

Data sovereignty and jurisdictional challenges in cross-cloud forensic investigations; Ethical constraints of attempting to de-anonymize Tor users in forensic contexts; Accuracy limitations of ML-based dark web traffic classification; Privacy and compliance obligations (GDPR, CCPA) when retaining cloud network logs; Responsibility of forensic investigators in presenting probabilistic network attribution evidence in legal proceedings.

Course Outcomes		
Course Outcomes (COs)	**Description**	**Bloom's Taxonomy Level**
At the end of the course the student will be able to:		
1	Explain the principles of network forensics, legal frameworks, and traffic capture techniques for preserving and analyzing network-based digital evidence.	**L2**
2	Apply deep packet inspection and protocol-level analysis to reconstruct network sessions.	**L3**
3	Analyze IDS/IPS alerts, firewall logs, and router syslogs to identify intrusion patterns.	**L4**

4	Analyze wireless and encrypted network traffic using forensic tools.	**L4**
5	Analyze cloud network flow logs and identify dark web traffic indicators.	**L4**

Table: Mapping Levels of COs to POs / PSOs

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	2	2	1	-	-	-	-	-	-	-	1	2	2
CO2	2	2	1	-	1	-	-	-	-	-	1	2	2
CO3	3	2	2	1	1	2	1	-	2	1	1	2	2
CO4	3	2	1	1	1	2	1	-	2	1	1	2	2
CO5	3	3	2	1	1	2	1	-	2	1	1	2	2

3: Substantial (High) 2: Moderate (Medium) 1: Poor (Low)

TEXT BOOKS:

1. Network Forensics: Tracking Hackers through Cyberspace – Sherri Davidoff & Jonathan Ham, Prentice Hall, 1st Edition, 2012.
2. The Practice of Network Security Monitoring – Richard Bejtlich, No Starch Press, 1st Edition, 2013.

REFERENCE BOOKS:

1. Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide – Laura Chappell, Protocol Analysis Institute, 2nd Edition, 2012.
2. Applied Network Security Monitoring: Collection, Detection, and Analysis – Chris Sanders & Jason Smith, Syngress, 1st Edition, 2013.

RECOMMENDED TOOLS:

Packet Capture & Analysis: Wireshark, tshark, tcpdump, Scapy, PyShark
Network Flow Analysis: Zeek (Bro), Argus, nfdump/nfsen, SiLK, Ntopng
Intrusion Detection & Log Analysis: Snort, Suricata, ELK Stack (Elasticsearch, Logstash, Kibana), Splunk, Graylog
Wireless Forensics: Aircrack-ng suite, Kismet, Wireshark (802.11), Ubertooth One
Network Reconstruction & Case Management: NetworkMiner, Xplico, CapLoader, ChaosReader
Scripting & Automation: Python (Scapy, PyShark, dpkt), Jupyter Notebook, Zeek Scripting Framework
AI Assistants: GitHub Copilot, ChatGPT, Claude

BIG DATA SECURITY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VII

Course Code	:		**Credits**	:	03
Hours / Week	:	03	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

To develop a strong foundation in securing big data systems by integrating cybersecurity principles, distributed architectures, and artificial intelligence techniques, enabling students to design intelligent, scalable, and secure data-driven infrastructures.

Course Objectives:

This course will enable students:

1. Understand the characteristics, types, and security concerns inherent in big data systems anc
2. Apply big data tools and technologies including Hadoop, Hive, MongoDB, and analytical frameworks to address data security challenges.
3. Analyze distributed big data architectures and evaluate security mechanisms for storage, computation, and stream processing.
4. Design and implement privacy-preserving techniques and security-by-distribution approaches to protect sensitive big data.
5. Integrate AI and machine learning techniques for anomaly detection, threat intelligence, and intelligent security decision-making in big data pipelines.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with traditional lecture method, different types of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I	**09 Hours**

Fundamentals of Big Data and Security

Topics: Introduction to Big Data: definition, evolution, and significance; Characteristics of Big Data: Volume, Velocity, Variety, Veracity, Value (5Vs); Types of Big Data: structured, semi-structured, unstructured; Operational Data Services for Big Data: batch, real-time, and hybrid processing models; Big Data Security Concerns: confidentiality, integrity, availability challenges; Big Data Security Challenges: data provenance, access control, secure multi-tenancy, insider threats, and compliance; Overview of big data security frameworks and standards.

Applications: Healthcare analytics security, financial fraud detection pipelines, enterprise log management, e-commerce transaction security.

AI Integration: AI-driven data classification and labelling, intelligent risk scoring for big data assets, automated security policy recommendation.

Authentic Intelligence: Responsible data stewardship: ethics of large-scale data collection; risks of re-identification from anonymised datasets; accountability in big data security decisions.

Relevant Online Resources (Relevant to this Module):

1. **Big Data Security — Coursera / edX Foundations** (4 hrs) | Path: Big Data Specialization — UC San Diego (Coursera)

   https://www.coursera.org/specializations/big-data

2. **Introduction to Hadoop Security — Apache Hadoop Official Docs** (Self-paced) | Path: Apache Hadoop Security Documentation

   https://hadoop.apache.org/docs/stable/hadoop-project-dist/hadoop-common/SecureMode.html

MODULE – II	**09 Hours**

Big Data Tools, Technologies and Data Protection

Topics: Big Data Tools Overview: reaching and processing big data; Issues, controversies, and problems in big data management; Data Science Analytical Tools: Hadoop ecosystem (HDFS, MapReduce), Hive (HiveQL, metastore, partitioning, bucketing), MongoDB (document model, CRUD, indexing, aggregation pipelines); Libraries, utilities; Data Protection strategies: encryption at rest and in transit, data masking, tokenisation, role-based access control (RBAC), attribute-based access control (ABAC); Secure data ingestion and pipeline integrity.

Applications: Enterprise data warehousing security, healthcare data lake protection, e-commerce personalisation with privacy, secure log analytics with Hive.

AI Integration: AI-assisted query optimisation in Hive, anomaly detection on MongoDB access logs, intelligent data masking using ML classification.

Authentic Intelligence: Responsible use of open-source tools: understanding licensing and community security disclosures; ethical implications of data retention policies in big data systems.

MODULE – III	**09 Hours**

Big Data Architecture, Storage and Distributed Security

Topics: Big Data Technologies: collection, storage, computation, stream processing, and data mining; Storage security: Hadoop Distributed File System (HDFS) internals and security; NoSQL Data Stores: HBase architecture and access control; Hadoop security model: Kerberos authentication, HDFS ACLs, wire encryption, data-at-rest encryption (HDFS TDE); Hadoop using Docker containers: containerised cluster setup and network isolation; Security-by-Distribution: managing big data in a federation of untrustworthy clouds; Distributed access control models; Monitoring and auditing in distributed systems: Apache Ranger, Apache Atlas.

Applications: Distributed log analysis for security auditing, containerised Hadoop deployments for secure multi-tenancy, federated data access across untrusted nodes.

AI Integration: ML-based anomaly detection on HDFS access logs, AI-driven audit trail analysis, intelligent Ranger policy recommendation..

Authentic Intelligence: Evaluating trade-offs between distribution and security in federated systems; ethical responsibilities of administrators managing distributed sensitive datasets.

MODULE – IV	**09 Hours**

Privacy Preservation in Big Data

Topics: Privacy preserving in big data: definitions, models, and goals; Privacy attacks: linkage attacks, inference attacks, membership inference, data poisoning; Privacy technologies: k-anonymity, l-diversity, t-closeness, differential privacy; Privacy metrics: information loss, disclosure risk, utility-privacy trade-off; Privacy-preserving data mining on unstructured data; Privacy-preserving analysis for big data using cryptographic tools: homomorphic encryption, secure multi-party computation (SMPC), federated learning; Regulatory compliance: GDPR, DPDP Act 2023, HIPAA implications for big data privacy.

Applications: Healthcare record de-identification, social media sentiment analysis with privacy, financial data anonymisation for analytics, federated learning in banking.

AI Integration: Differential privacy implementation using Python (Google DP library), federated learning simulations with PySyft, AI-driven privacy risk scoring.

Authentic Intelligence: Ethical limits of data anonymisation; risks of re-identification even in anonymised datasets; responsible use of cryptographic privacy tools in research and commercial settings.

1. **Hadoop Security — Ben Spivey & Joey Echeverria** (2 hrs) | Path: O'Reilly Media — Apache Hadoop Security Documentation
   https://www.oreilly.com/library/view/hadoop-security/9781491900970/

MODULE – V	**09 Hours**

AI-Based Big Data Security and Threat Intelligence

Topics: AI in big data cybersecurity: supervised and unsupervised learning for threat detection; Anomaly detection techniques: statistical methods, Isolation Forest, Autoencoders, LSTM for sequential log analysis;

Risk-based authentication systems; Security analytics and predictive models on big data streams; Trust and reputation systems in distributed data environments; Intrusion Detection Systems (IDS) for big data platforms (Hadoop, Hive, MongoDB); Big data security monitoring: Apache Metron, real-time threat intelligence pipelines; Autonomous security response using SOAR on big data events; Ethical AI and human oversight in automated security decisions.

Applications: Network intrusion detection on large-scale traffic logs, fraud detection in financial big data systems, social media threat intelligence, healthcare anomaly detection.

AI Integration: LSTM-based log anomaly detection, Isolation Forest for big data outlier detection, federated threat intelligence sharing.

Authentic Intelligence: Avoiding algorithmic bias in AI-driven security decisions; ethical obligations when AI systems flag false positives; human oversight mandates in autonomous big data security response.

Relevant Online Resources (Relevant to this Module):

1. **Big Data Security Analytics — Apache Metron / Splunk** (Self-paced) | Path: O'Reilly Media — Apache Metron Project Documentation & Splunk Free Training

https://metron.apache.org/ https://www.splunk.com/en_us/training.html

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Explain the characteristics, types, and security challenges of big data systems and evaluate applicable security frameworks.	L2
2	Apply big data tools — Hadoop, Hive, and MongoDB — to build and secure data processing pipelines.	L3
3	Design secure distributed big data architectures using HDFS, HBase, Kerberos, Apache Ranger, and containerised deployments.	L3
4	Implement privacy-preserving techniques including differential privacy, k-anonymity, and cryptographic tools in big data analytics.	L3

5	Apply AI and ML techniques for anomaly detection, intrusion detection, and intelligent threat response in big data security systems.	L5

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	2	2	1	-	-	-	-	-	-	-	1	2	2
CO2	2	2	1	-	-	-	-	-	-	-	1	2	2
CO3	3	2	1	1	1	2	1	-	2	1	1	2	2
CO4	3	2	1	1	1	2	1	-	2	1	1	2	2
CO5	3	2	1	1	1	2	1	-	2	1	1	2	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Cloud Security: A Comprehensive Guide to Secure Cloud Computing – Ronald L. Krutz & Russell Dean Vines, Wiley, 1st Edition, 2010.
2. Big Data: A Revolution That Will Transform How We Live, Work, and Think – Viktor Mayer-Schönberger & Kenneth Cukier, Houghton Mifflin Harcourt, 2013.

REFERENCE BOOKS:

1. Data Security in Cloud Computing – Rajeev Kanth, CRC Press, 2019.
2. Hadoop: The Definitive Guide – Tom White, O'Reilly Media, 4th Edition, 2015.

RECOMMENDED TOOLS:

1. Big Data Frameworks: Apache Hadoop, Apache Hive, HBase, Apache Spark
2. Databases & Storage: MongoDB, Apache Cassandra, HDFS, Amazon S3
3. Security Tools: Apache Ranger, Apache Knox, Apache Atlas, Kerberos
4. Privacy & Compliance: Google Differential Privacy Library, PySyft (OpenMined), ARX Data Anonymisation
5. AI/ML & Analytics: Python (Scikit-learn, TensorFlow), Apache Metron, Splunk, ELK Stack

SECURITY ENGINEERING AND CYBER DEFENCE

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VII

Course Code	:		**Credits**	03
Hours / Week	:	3	**Total Hours**	**45**
L–T–P–J	:	3–0–2–0	**CIE+SEE**	60+40 Marks

Course Vision:

To develop competent professionals capable of designing, implementing, and managing secure systems and cyber defense strategies that protect organizational assets against evolving cyber threats, while ensuring confidentiality, integrity, and availability, and aligning with industry standards and best practices.

Course Objectives:

This course will enable students:

1.Understand fundamental concepts of Security Engineering and Cyber Defense.

2.Learn core security goals such as CIA Triad (Confidentiality, Integrity, Availability).

3.Study cryptographic techniques and secure communication methods.

4.Analyze system, network, and endpoint security mechanisms.

5. Apply authentication, authorization, and access control models.

6. Understand cyber threats, malware, and Defense mechanisms.

7. Develop skills in network security tools such as firewalls, IDS/IPS, and VPNs.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with traditional lecture method, different types of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.

Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I	**09 Hours**

INTRODUCTION TO SECURITY ENGINEERING

Topics: Introduction to security engineering, Security goals: Confidentiality, Integrity, Availability (CIA Triad), Threats, vulnerabilities, and risk management, Types of cyber-attacks (malware, phishing, ransomware), Security principles and policies, Basics of Cryptography.

Applications: Identifying risks in organizations (risk assessment), Designing basic security policies.

AI Integration: AI analyzes large volumes of logs and network traffic, detects unusual patterns (anomalies) in real time, Identifies malware, phishing, and ransomware early.

Authentic Intelligence: Introduction to security engineering, Security goals: Confidentiality, Integrity, Availability (CIA Triad), Threats, vulnerabilities, and risk management, Types of cyber-attacks (malware, phishing, ransomware), Security principles and policies, Basics of Cryptography.

MODULE – II	**09 Hours**

Cryptography & Secure Communication

Topics: Definition and importance of cryptography, Goals of cryptography (confidentiality, integrity, authentication), Types of attacks on cryptographic systems, Symmetric Key Cryptography, Asymmetric Key Cryptography, Hash Functions, Digital Signatures, Secure Communication Protocols.

Applications: Protects data sent over the internet using encryption (HTTPS, SSL/TLS),

Ensures safe browsing, messaging, and email communication, Prevents eavesdropping and data theft.

AI Integration: AI detects **brute force, cryptanalysis, and pattern-based attacks,** identifies abnormal encryption/decryption attempts, Learns attack patterns from historical data.

Authentic Intelligence: Identifies attacks like brute force or cryptanalysis, clearly explains *why* an activity is flagged.

MODULE – III	**09 Hours**

System & Endpoint Security Engineering

Topics: Operating System Security, Authentication & Authorization, Access Control Models, Malware Protection, Logging and Monitoring, Mobile & Device Security.

Applications: Secures employee laptops, desktops, and workstations, prevents unauthorized access and data leakage, Protects ATM systems and banking servers, secures customer login systems, Ensures safe use of corporate systems.

AI Integration: AI monitors system behaviour continuously, detects malware, ransomware, and unknown threats (zero-day attacks) , AI improves endpoint security tools.

Authentic Intelligence: Identifies malware, ransomware, and suspicious processes, clearly explains the reason for detection, Uses verified system behavior and logs

MODULE – IV	**09 Hours**

Cyber Defense Fundamentals

Topics:

Authentication and authorization mechanisms, Multi-Factor Authentication (MFA) ,Role-Based Access Control (RBAC) ,Preventing unauthorized access, Firewalls (hardware & software), Intrusion Detection & Prevention Systems (IDS/IPS) ,Network segmentation, VPN and secure communication, Antivirus and anti-malware systems , Endpoint Detection and Response (EDR) ,System hardening techniques ,Device encryption and patch management, Malware Defense.

Applications:

Protects company computers, servers, and internal networks, prevents malware infection in business environments, Ensures secure workplace operations

AI Integration: AI analyzes files, programs, and system behaviour, detects known and unknown malware (zero-day threats), Uses pattern recognition and machine learning

Authentic Intelligence: Identifies malware using behaviour and file analysis, clearly explains detection results, Builds trust in security decisions.

MODULE – V	09 Hours
Network Security & Cryptographic Protection **Topics:** Firewalls & Network Perimeter Security, Intrusion Detection & Prevention Systems (IDS/IPS), Cryptographic Protection in Networks, Secure Communication Protocols, Public Key Infrastructure (PKI), Network Attacks & Defense, Network Monitoring & Logging. **Applications:** Protects data during browsing, emailing, and messaging, Uses HTTPS, SSL/TLS encryption, Prevents interception of sensitive data. **AI Integration:**Detects abnormal network traffic patterns, identifies cyber-attacks in real time, Improves IDS/IPS systems. **Authentic Intelligence:** Detects attacks like MITM, DDoS, spoofing, clearly explains the reason behind alerts, Uses verified network logs and traffic patterns.	

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Explain the fundamentals of Security Engineering, CIA Triad, threats, vulnerabilities, and risk management.	L2
2	Apply cryptographic techniques including symmetric, asymmetric encryption, hashing, and digital signatures.	L3
3	Analyze operating system security, authentication, authorization, and access control mechanisms.	L4
4	Explain network security mechanisms such as firewalls, IDS/IPS, VPN, and endpoint security tools.	L2
5	Apply security monitoring, logging, and incident response techniques for real-world cyber defense.	L2

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs													
COs	**Program Outcomes (POs)**											**PSOs**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**1**	**2**
CO1	3	1	2	2	3	1		1	2	2		2	2
CO2	3	1	2	2	3	1		1	2	2		2	2
CO3	3	1	2	2	3	1		1	2	2		2	2
CO4	3	1	2	2	3	1		1	2	2		2	2
CO5	3	1	2	2	3	1		1	2	2		2	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd ed. Hoboken, NJ, USA: John Wiley & Sons, 2020, ISBN: 978-1119642787.
2. D. G. Firesmith, *Common System and Software Security Weaknesses and Mitigation Guidelines*, 1st ed. Upper Saddle River, NJ, USA: Addison-Wesley, 2010.
3. Y. Diogenes and E. Ozkaya, *Cybersecurity: Attack and Defense Strategies*, 2nd ed. Birmingham, UK: Packt Publishing, 2018.

REFERENCE BOOKS:

1. 1. N. R. Mead, C. Woody, and J. A. Haller, *Cyber Security Engineering: A Practical Approach for Systems and Software Assurance*, 1st ed. Boston, MA, USA: Addison-Wesley, 2016.
2. W. Easttom, *Network Defense and Countermeasures: Principles and Practices*, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall, 2013.

Recommended Tools:

- Wazuh (central monitoring)
- Suricata (network detection)
- Kibana (dashboard)
- Wireshark (deep inspection)
- Python (automation)

GENERATIVE AI AND LARGE LANGUAGE MODELS

[As per Choice Based Credit System (CBCS) Scheme]

SEMESTER – VII

Course Code	:		Credits	:	03
Hours / Week	:	03	Total Hours	:	45
L–T–P–J	:	3–0–0–0	CIE + SEE	:	60+40 Marks

Course Vision: To equip students with a strong conceptual and hands-on foundation in Generative AI and Large Language Models — covering core architectures, modern LLMs, diffusion models, prompt engineering, and applied deployment — so they can design, evaluate, and responsibly deploy generative AI applications.

Course Objectives: This course will enable students:

- Understand the principles of generative modelling and distinguish generative from discriminative approaches.
- Explore core architectures — AutoEncoders, VAEs, GANs, and Transformers — that underpin modern Generative AI.
- Examine how Large Language Models (BERT, GPT, T5, LLaMA) are pre-trained, fine-tuned, and evaluated.
- Apply prompt engineering techniques — zero-shot, few-shot, chain-of-thought — to steer LLM outputs effectively.
- Build LLM-powered applications using RAG pipelines, LangChain, and NVIDIA NIM/NeMo tools. Appreciate the ethical considerations, bias, fairness, and responsible deployment practices for generative AI systems.

Teaching-Learning Process (General Instructions)

These are sample pedagogical methods teachers can adopt to develop course outcomes:

Lecture Method: Core concepts explained with real-world examples, architecture diagrams, and case studies.

- Interactive Teaching: Live demos of ChatGPT, DALL·E, Stable Diffusion; group discussion on GenAI use cases and risks.
- Video/Animation: NVIDIA DLI course videos and visual walkthroughs of transformer attention mechanisms.
- Collaborative Learning: Pair labs for prompt engineering experiments and RAG pipeline construction.
- Hands-On Coding: NVIDIA DLI Jupyter notebooks using GPU-accelerated Google Colab environments.

MODULE – I: Foundations of Generative AI	09 Hours

Topics: What is Generative AI? Generative vs. Discriminative modelling — key differences with examples; Historical perspective: rule-based systems - GANs- Transformers-LLMs -Multimodal models; Overview of application areas: text, image, audio, video, and code generation; Limitations and risks: hallucinations, deepfakes, copyright concerns, and over-reliance; Pre-training and Transfer Learning: why foundation models generalise across tasks; Ethics, bias, and fairness in Generative AI: sources of bias and mitigation strategies.

Applications: ChatGPT generating confident but factually incorrect answers (hallucination); DALL·E 3 creating images from text prompts for content creation workflows; GitHub Copilot using pre-trained code models to assist developers in real time.

AI Integration: Explore the NVIDIA 'Generative AI Explained' free DLI course interactively; compare outputs of a discriminative classifier vs. a generative model on the same dataset using a Colab notebook; document three real-world GenAI use cases with their risks.

Authentic Intelligence: Understanding of transformers and assessing ethics and bias.

MODULE – II: Core Generative Architectures & Word Representations	09 Hours

Topics: Word Embeddings and Tokenisation: how language is numerically represented; Word2Vec, GloVe, byte-pair encoding (BPE); AutoEncoders: encoder-decoder architecture, bottleneck representation, unsupervised feature learning; Variational AutoEncoders (VAEs): probabilistic latent space, reparameterisation trick, applications in image generation; Generative Adversarial Networks (GANs): generator vs. discriminator, training dynamics, mode collapse; Evaluation metrics: FID (Frechet Inception Distance), BLEU, ROUGE; Comparison of VAEs vs. GANs vs. Diffusion Models: trade-offs in quality, diversity, and training stability.

Applications: VAE-based face image generation and latent space interpolation; GAN-based synthetic data generation for medical imaging and data augmentation; Word embeddings powering semantic search in document retrieval systems.

AI Integration: Implement a simple VAE on MNIST using PyTorch on Google Colab; visualise the 2D latent space; interpolate between two digit classes; compute FID score to evaluate generated image quality; compare with a basic GAN on the same dataset.

Authentic Intelligence: Insights into VAEs and GANs

MODULE – III: The Transformer Architecture	09 Hours

Topics: Evolution to Transformers: limitations of RNNs and LSTMs; why sequence modelling needed a new approach; Self-Attention mechanism: query, key, value matrices; scaled dot-product attention computation; Multi-Head Attention: parallel attention heads and what each head learns; Positional Encoding: sinusoidal and learned encodings; why position matters in text; Encoder-Decoder structure: encoder-only (BERT), decoder-only (GPT), and encoder-decoder (T5) variants; Vision Transformers (ViT): applying the transformer architecture to image patches; Transformer applications: machine translation, text summarisation, question answering, image classification.

Applications: Google Translate powered by Transformer encoder-decoder models; ViT applied to medical image classification outperforming CNN baselines; BERT-based semantic similarity used in search engines for query understanding.

AI Integration: Implement a simplified self-attention layer in PyTorch on Google Colab; visualise attention weights for a short sentence; use Hugging Face BertViz to inspect multi-head attention in a pre-trained BERT model.

Authentic Intelligence: Analyze and understand the concepts of transformers

MODULE – IV: Large Language Models (LLMs)	09 Hours

Topics: BERT: masked language modelling, next sentence prediction, fine-tuning for NLP classification tasks; GPT family: autoregressive language modelling, GPT-2, GPT-3, GPT-4 — capabilities and differences; T5: Text-to-Text Transfer Transformer — unified framework for all NLP tasks; LLM Scaling Laws: LLM Families overview: LLaMA, Mistral, Gemma — open-source vs. proprietary models; Prompt Engineering: zero-shot, few-shot, chain-of-thought, and self-consistency prompting techniques; RLHF (Reinforcement Learning from Human Feedback): how ChatGPT-style alignment works — conceptual overview.

Applications: BERT fine-tuned for sentiment analysis on product reviews; GPT-4 powering customer support chatbots with multi-turn dialogue; T5 used for abstractive summarisation of news articles.

AI Integration: Fine-tune bert-base-uncased from Hugging Face on an IMDB sentiment classification task on Google Colab; compare zero-shot vs. few-shot GPT prompting for a

question-answering task; experiment with chain-of-thought prompting on a reasoning benchmark using NVIDIA NIM API. **Authentic Intelligence**: Conceptual knowledge about prompt engineering and its types	
MODULE – V: Advanced Generative Models and Applied LLM Engineering	09 Hours
Topics: Diffusion Models: forward and reverse diffusion process, denoising diffusion probabilistic models (DDPM); UNet architecture in diffusion models; role of the noise predictor at each timestep; Latent Diffusion Models (LDMs) and Stable Diffusion — efficient generation in latent space; DALL·E 2 and Transformer-based image generation pipelines; Multimodal Learning: CLIP — connecting text and images; BLIP for visual question answering; RAG (Retrieval-Augmented Generation): grounding LLM outputs with external knowledge; vector databases (FAISS, ChromaDB); Introduction to LLM Agents and tool use: LangChain basics, function calling, agentic workflows (awareness level); Responsible deployment. **Applications:** Stable Diffusion generating product visualisations for e-commerce from text descriptions; RAG-based enterprise chatbot grounding answers in a company knowledge base to reduce hallucinations; CLIP-based multimodal search enabling image retrieval using natural language queries. **AI Integration:** Run a Stable Diffusion pipeline on Google Colab using Hugging Face Diffusers; build a simple RAG chatbot with LangChain and FAISS over a small document set using NVIDIA NIM; configure a basic NeMo Guardrails output filter and test hallucination scenarios. **Authentic Intelligence:** Overview of vector databases and diffusion models	

Course Outcome		
CO	**At the end of the course the student will be able to:**	**Bloom's Taxonomy Level**
1	Explain the principles of generative modelling, describe the architecture of AutoEncoders, VAEs, and GANs, and compare them with discriminative models.	L2
2	Describe the Transformer architecture — self-attention, multi-head attention, and positional encoding — and explain how these components enable modern LLMs.	L2

3	Summarise how BERT, GPT, and T5 are pre-trained and fine-tuned; apply prompt engineering techniques (zero-shot, few-shot, chain-of-thought) to steer LLM outputs effectively.	L3
4	Build a simple RAG pipeline using LangChain and a vector database to ground LLM responses in external knowledge, and evaluate output quality using BLEU/ROUGE metrics.	L3
5	Analyze ethical considerations, bias, hallucination risks, and responsible deployment practices for generative AI systems, including RLHF and guardrail frameworks.	L4

Table: Mapping Levels of COs to POs / PSOs

COs	1	2	3	4	5	6	7	8	9	10	11	PSO 1	PSO 2
CO1	3	2	1	-	-	2	-	-	2	-	1	2	2
CO2	3	3	2	1	-	2	1	-	2	-	1	2	2
CO3	3	3	2	2	1	2	1	1	2	1	1	3	2
CO4	3	2	2	2	1	2	1	1	2	1	1	2	3
CO5	2	2	1	1	2	3	2	1	3	1	2	2	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

- Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press. deeplearningbook.org. (Ch. 14, 20 — Autoencoders, GANs, Generative Models)

- Foster, D. (2023). Generative Deep Learning (2nd ed.). O'Reilly Media. (Comprehensive coverage of VAEs, GANs, Diffusion Models, Transformers, LLMs)

- Tunstall, L., von Werra, L., & Wolf, T. (2022). Natural Language Processing with Transformers. O'Reilly Media. (BERT, GPT, T5, fine-tuning, deployment)

- NVIDIA Deep Learning Institute. (2024). Generative AI Teaching Kit. developer.nvidia.com/teaching-kits. (Modules 1–6 — core course reference)

REFERENCE BOOKS:

- Vaswani, A. et al. (2017). Attention Is All You Need. NeurIPS. arXiv:1706.03762.

- Ho, J., Jain, A., & Abbeel, P. (2020). Denoising Diffusion Probabilistic Models. NeurIPS. arXiv:2006.11239.

- Devlin, J. et al. (2018). BERT: Pre-training of Deep Bidirectional Transformers. arXiv:1810.04805.

- Brown, T. et al. (2020). Language Models are Few-Shot Learners (GPT-3). NeurIPS. arXiv:2005.14165.

- Radford, A. et al. (2021). Learning Transferable Visual Models from Natural Language Supervision (CLIP). ICML.

RECOMMENDED TOOLS & FRAMEWORKS

- Hugging Face Transformers & Diffusers — pre-trained BERT, GPT, T5, Stable Diffusion pipelines (huggingface.co)

- LangChain / LangGraph — LLM application development, RAG pipelines, and agentic workflows

- NVIDIA NIM Microservices — inference API for LLaMA, Mistral, and other open models (build.nvidia.com)

- NVIDIA NeMo Guardrails — output filtering, hallucination mitigation, responsible AI deployment (developer.nvidia.com/nemo-guardrails)

- FAISS / ChromaDB — vector databases for RAG pipeline construction

- OpenAI CLIP — multimodal text-image embedding and retrieval

- Programming: Python 3 (PyTorch, scikit-learn) — Google Colab / Jupyter (NVIDIA GPU-enabled)

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

AI POWERED DATA CENTRE SECURITY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VII

Course Code	:		**Credits**	:	03
Hours / Week	:	03	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE + SEE**	:	60 + 40 Marks

Course Vision: To equip students with advanced knowledge of AI-driven security frameworks for modern data centres, enabling them to architect, deploy, and manage intelligent, self-adaptive security systems that ensure confidentiality, integrity, availability, and ethical compliance across hybrid and cloud-native environments.

Course Objectives: This course will enable students to:

- Understand AI-augmented data centre architectures, threat landscapes, and security paradigms.
- Design AI-integrated physical and environmental security systems for critical infrastructure.
- Apply AI-driven network, virtualization, and software-defined security controls.
- Implement intelligent data protection, risk management, and compliance automation frameworks.
- Integrate advanced AI/ML security solutions with Zero Trust architecture in hybrid environments.

Teaching-Learning Process (General Instructions)

Pedagogical methods to accelerate course outcome attainment:

- Lecture method along with interactive demonstrations of AI security tools and real-time dashboards.
- Interactive Teaching: brainstorming, case-study discussions, threat simulation exercises, and role-playing red/blue team scenarios.
- Video/Animation films illustrating AI-based intrusion detection, autonomous response systems, and anomaly visualisation.
- Collaborative (Group Learning): team-based labs on building AI models for threat detection and SIEM configuration.
- Critical Thinking: HOT-level quiz questions, design challenges, and hands-on projects with AI security platforms.
- Encourage students to propose novel AI-powered security architectures and benchmark multiple approaches.

MODULE – I: AI-Augmented Data Centre Infrastructure & Security Fundamentals	**9 Hours**

Topics: Data Centre Essentials: Definitions, evolution (traditional → cloud-native → AI-driven), Tier Architecture (TIA-942 Tiers I–IV). The AI Security Mandate: CIA triad extended with AI dimensions (model integrity, data poisoning, adversarial attacks). Modern Threat Landscape: Physical intrusions, environmental risks, cyberattacks (DDoS, ransomware, APTs), supply-chain attacks, adversarial ML threats. AI Foundations for Security:

Supervised/unsupervised learning, anomaly detection algorithms, NLP for log analysis, reinforcement learning for adaptive defence. Standardisation: TIA-942, Uptime Institute, NIST AI RMF.

Applications: Critical infrastructure design augmented by AI monitoring, intelligent SLA management, AI-driven anomaly detection for cloud and colocation facilities.

AI Integration: Predictive maintenance for cooling/power systems using ML, AI-based anomaly detection in operations and traffic, LLM-assisted threat intelligence synthesis, digital twin simulation for security stress-testing.

Authentic Intelligence: Human-in-the-loop decision-making for high-availability systems; ethical considerations in AI deployment — data sovereignty, bias in threat scoring, explainability requirements.

Relevant Online Resources (Relevant to this Module):

1. NIST AI Risk Management Framework https://www.nist.gov/artificial-intelligence

2. Introduction to Data Center Infrastructure Security https://www.coursera.org/learn/data-center-security-management-with-microsoft-system-center

MODULE – II: AI-Driven Physical Security & Intelligent Environmental Controls	**9 Hours**

Topics: Layered Perimeter Defence: Fencing, bollards, lighting, guard stations, mantraps. Advanced AI-Enhanced Access Control: Biometrics (iris/fingerprint/facial recognition with liveness detection), smart cards, RFID, AI-powered visitor management. Intelligent Environmental Monitoring: AI-based fire suppression triggers, HVAC optimisation via RL agents, leak and thermal anomaly detection. Smart Asset Protection: AI-enabled CCTV with behavioural analytics, RFID asset tracking with ML-based loss prevention, secure decommissioning verification.

Applications: Automated intrusion response systems, predictive environmental risk mitigation, AI-assisted physical audit trails, smart building security integration.

AI Integration: Computer vision for real-time surveillance and unauthorised-access detection, ML models for thermal anomaly classification, AI-based biometric anti-spoofing, reinforcement learning for HVAC optimisation and energy-efficient security.

Authentic Intelligence: Privacy implications of AI surveillance (GDPR compliance); bias in facial recognition systems; accountability frameworks for automated physical security decisions.

Relevant Online Resources (Relevant to this Module):

1. AI Video Surveillance and Ethics https://www.coursera.org/learn/introduction-to-ai-in-physical-security 2. RFID and IoT Security for Data Centres https://www.edx.org/course/iot-security

MODULE – III: AI-Powered Logical, Network & Virtualisation Security	**9 Hours**

Topics: AI-Enhanced Network Defences: NGFW with ML-driven rule generation, AI-powered IDS/IPS, micro-segmentation (East-West traffic). Virtualisation Security: Hypervisor hardening with AI monitoring, guest OS isolation, secure AI-orchestrated VM migration. Software-Defined Infrastructure: Security in SDN/NFV with AI policy enforcement, VXLAN threat detection. AI for Vulnerability Management: Automated penetration testing (autoPT), AI-driven CVE prioritisation, graph-neural-network-based lateral movement detection.

Applications: Customer-adaptive network segmentation, real-time anomaly detection in virtualised workloads, AI-powered traffic pattern classification for zero-day detection.

AI Integration: Deep learning for encrypted traffic analysis, AI-driven intrusion detection and automated containment, GNN-based lateral movement detection, LLM-assisted vulnerability report triage.

Authentic Intelligence: Risks of over-automation in security enforcement; responsible AI in network access decisions; transparency in ML-driven firewall rules.

Relevant Online Resources (Relevant to this Module):

1. Network Intrusion Detection with Machine Learning https://www.coursera.org/learn/introduction-to-intrusion-detection-systems-ids 2. AI in Cybersecurity Specialization https://www.coursera.org/specializations/ai-cybersecurity

MODULE – IV: Intelligent Storage Security, Risk Management & Compliance Automation	**9 Hours**

Topics: AI-Driven Data Protection: Encryption at rest (AES-256) and in transit (mTLS, IPsec) with AI key-lifecycle management. Storage Security: SAN/NAS hardening (LUN masking, zoning) with ML-based access anomaly detection. Compliance Automation: ISO/IEC 27001, SOC 2, PCI DSS, GDPR with AI compliance monitoring bots. Business Continuity: AI-assisted DR orchestration, predictive RTO/RPO modelling, automated incident response playbooks. AI-Enhanced Auditing: NLP-powered log analysis, next-gen SIEM with ML correlation, automated compliance reporting.

Applications: Financial and healthcare data protection with automated compliance checks, AI-driven forensic analysis, predictive risk scoring for data assets.

AI Integration: ML-based log anomaly detection and SIEM correlation, predictive risk assessment models, NLP for automated audit report generation, AI-powered encryption key anomaly detection.

Authentic Intelligence: Ethical handling of sensitive personal data in AI systems; accountability for automated compliance decisions; explainability in AI-driven risk scoring.

Relevant Online Resources (Relevant to this Module):

1. AI-Powered SIEM and Log Analysis https://www.splunk.com/en_us/training.html 2. GDPR and AI Compliance https://www.edx.org/course/gdpr-and-ai

MODULE – V: AI Security Administration, Zero Trust & Hybrid Best Practices	**9 Hours**

Topics: AI-Augmented System Management: Server cluster security with AI health monitoring, autonomous patch orchestration, configuration drift detection. Cloud-Native AI Security: Hybrid/multi-cloud AI security posture management (AI-CSPM), CASB with ML anomaly detection. Zero Trust Architecture (ZTA) with AI: Continuous adaptive PEP/PDP engines, AI-driven identity verification, self-healing micro-perimeters. AI Governance & Documentation: Responsible AI policy for security automation, SOPs, SLAs, audit logs, bias audits, explainability requirements. Emerging Frontiers: Quantum-safe cryptography, AI-versus-AI adversarial scenarios, autonomous SOC concepts.

Applications: Hybrid cloud AI security governance, enterprise security automation pipelines, self-healing infrastructure deployment, quantum-readiness assessment.

AI Integration: AI-enhanced SIEM for alert prioritisation and noise reduction, autonomous patch and configuration management, RL-based self-healing infrastructure, LLM-powered SOC analyst assistants.

Authentic Intelligence: Addressing algorithmic bias in AI-driven threat detection; organisational responsibility in deploying autonomous security systems; human oversight requirements for AI SOC decisions.

Relevant Online Resources (Relevant to this Module):

1. Zero Trust Architecture and AI https://www.nist.gov/publications/zero-trust-architecture 2. AI for Security Operations https://www.coursera.org/learn/ai-for-cybersecurity

Course Outcomes

CO	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
CO1	Analyse AI-augmented data centre architectures (TIA-942 + AI RMF) and identify vulnerabilities including AI-specific attack vectors.	L4
CO2	Design AI-integrated physical and environmental security mechanisms incorporating computer vision and intelligent monitoring.	L6
CO3	Apply AI-powered network, virtualisation, and software-defined security controls with automated policy enforcement.	L3
CO4	Evaluate AI-driven storage security, automated compliance frameworks, and intelligent disaster recovery strategies.	L5
CO5	Implement advanced AI/ML security systems with Zero Trust Architecture and autonomous SOC capabilities in hybrid environments.	L6

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	3	3	2	-	-	-	-	-	-	-	1	2	2
CO2	3	3	2	1	1	-	-	1	-	1	1	3	2
CO3	3	2	2	2	2	2	1	-	2	1	1	3	2
CO4	3	2	2	2	1	2	2	1	2	1	1	2	3
CO5	3	3	2	2	2	3	2	1	2	2	2	3	3

3: Substantial (High) 2: Moderate (Medium) 1: Low

TEXT BOOKS:

- Mauricio Arregoces, Maurizio Portolani – Data Center Fundamentals, Cisco Press.
- Hwaiyu Geng – Data Center Handbook, Wiley.
- Charu C. Aggarwal – Artificial Intelligence: A Textbook, Springer.
- Mark Stamp – Introduction to Machine Learning with Applications in Information Security, CRC Press.

REFERENCE BOOKS:

- TIA-942 – Telecommunications Infrastructure Standard for Data Centers.
- William Stallings – Network Security Essentials, Pearson.
- Evan Gilman, Doug Barth – Zero Trust Networks, O'Reilly.
- NIST SP 800-207 – Zero Trust Architecture.
- NIST AI RMF 1.0 – AI Risk Management Framework.

RECOMMENDED TOOLS:

- Cisco Packet Tracer — for simulating AI-augmented data centre network topologies.
- Splunk / IBM QRadar — for AI-powered SIEM, log correlation, and threat detection labs.
- Snort / Suricata — for IDS/IPS with ML-based signature generation.
- Wireshark — for deep packet inspection and AI traffic classification experiments.
- Python (scikit-learn, TensorFlow, PyTorch) — for building and evaluating AI security models.
- AutoCAD / draw.io — for designing AI-integrated perimeter security blueprints.
- Nmap / OpenVAS — for network scanning and AI-assisted vulnerability prioritisation.

Mobile & IoT Forensics

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VII

Course Code	:		**Credits**	:	03
Hours / Week	:	03	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

To develop the ability to acquire, analyze, and investigate digital evidence from mobile and IoT devices using modern forensic tools and techniques while ensuring legal compliance and ethical practices.

Course Objectives:

This course will enable students:

1. To understand fundamentals of digital forensics and mobile ecosystems
2. To apply mobile forensic acquisition and analysis techniques
3. To analyze IoT architectures and perform IoT forensic investigations
4. To utilize forensic tools for evidence extraction and reconstruction
5. To evaluate legal, ethical, and security challenges in digital investigations

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. Lecture methods along with traditional lecture delivery may be adopted to explain fundamental concepts of Mobile and IoT Forensics effectively.
2. Interactive Teaching: incorporating brainstorming sessions, group discussions, focused listening, formulation of investigative questions, notetaking, annotation of digital evidence, and role-playing of real-world forensic investigation scenarios.
3. Showing video/animation films to demonstrate mobile forensic acquisition techniques, IoT data flow, and cybercrime case investigations.
4. Encourage Collaborative (Group Learning) in the class through team-based forensic analysis tasks and case study evaluations.
5. Demonstrations using forensic tools to provide hands-on exposure to mobile and IoT evidence acquisition and analysis techniques.
6. To develop critical thinking, asking Higher Order Thinking questions in the form of quizzes, scenario-based problem solving, and forensic analysis tasks involving complex datasets.

MODULE – I	**09 Hours**

Introduction to Mobile, IoT, and Social Media Forensics

Topics: Social Media Forensics: Social media evidence collection and preservation techniques; Investigation of digital evidence from platforms such as Facebook, Instagram, and X (Twitter); Preservation of online content and metadata for forensic investigations. Open-Source Intelligence (OSINT): Fundamentals of OSINT investigations; Information gathering from public sources; Username, email, and digital footprint analysis; Image verification and reverse image search techniques. Multimedia and Metadata Analysis: Image geo-tagging analysis; Metadata extraction from images and digital media; Timeline and location correlation techniques. Dark Web and Cyber Persona Investigation: Introduction to dark web investigations; Basic dark web navigation and threat awareness; Cyber persona profiling and attribution basics; Ethical and legal considerations in OSINT and social media investigations.

Applications: Cybercrime investigation and digital evidence handling, forensic analysis in criminal and civil cases, identification and preservation of digital evidence from mobile and IoT environments.

AI Integration: Introduction to AI-assisted forensic workflows, automated log analysis and evidence filtering using Python, use of data analytics tools for identifying patterns in digital evidence.

Authentic Intelligence: Understanding real-world constraints in forensic investigations, challenges in maintaining evidence integrity and chain of custody, risks of mishandling digital evidence, legal admissibility issues, and ethical responsibilities.

NVIDIA DLI Courses (Relevant to this Module):

1. Accelerating End-to-End Data Science Workflows (8 hrs) | Path: Data Science Training - Accelerated Data Science Foundations

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-01+V2

2. Best Practices in Feature Engineering for Tabular Data With GPU Acceleration (2 hrs) | Path: Accelerated Data Science Foundations

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-06+V1

MODULE – II	**09 Hours**

Mobile Device Forensics

Topics: Mobile Operating Systems (Android, iOS), File Systems, Mobile Data Storage, Logical and Physical Acquisition Techniques, SIM and Memory Analysis, Handling Encrypted and Locked Devices.

Applications: Extraction of data from mobile devices, recovery of deleted files, analysis of communication records and stored data.

AI Integration: Automated classification and filtering of mobile data, use of machine learning techniques to identify relevant evidence, data parsing using Python tools.

Authentic Intelligence: Risks in acquisition processes, challenges in dealing with encryption, privacy concerns, and maintaining forensic soundness.

MODULE – III	**09 Hours**

Mobile Data Analysis and Cloud Forensics

Topics: Analysis of Call Logs, SMS, Contacts, Multimedia Data, Application Data (WhatsApp, Telegram), Browser History, Timeline Reconstruction, Cloud Storage and Backup Analysis (Google Drive, iCloud).

Applications: User behavior analysis, communication tracking, reconstruction of events, cloud-based evidence investigation.

AI Integration: NLP techniques for message analysis, automated timeline generation, machine learning for correlating cloud and device data.

Authentic Intelligence: Risks of misinterpretation of user data, privacy and jurisdiction challenges in cloud forensics, ensuring accuracy of conclusions.

NVIDIA DLI Free Courses (Relevant to this Module):

1. **Accelerating Clustering Algorithms to Achieve the Highest Performance** (2 hrs) | Path: Data Science Training – Accelerated Data Science Foundations

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-04+V1

MODULE – IV	**09 Hours**

IoT Architecture and Forensic Acquisition

Topics: IoT Fundamentals, IoT Architecture Layers, Device Types, Communication Protocols (Wi-Fi, Bluetooth, Zigbee, MQTT), IoT Evidence Collection, Network Traffic Analysis, Firmware Extraction.

Applications: Investigation of smart home and industrial IoT systems, capturing device and network-based evidence, firmware analysis.

AI Integration: AI-based traffic analysis, anomaly detection in IoT communication, automated firmware analysis techniques.

Authentic Intelligence: Challenges due to heterogeneous devices, data volatility, lack of standardization, and limited access to proprietary systems.

NVIDIA DLI Courses (Relevant to this Module):

1. Big Data Security E**xploring Adversarial Machine Learning** (8 hrs) | Path: Deep Learning Training – AI Security Engineering & Federated ML

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-03+V1

MODULE – V	**09 Hours**

IoT Data Analysis, Security and Reporting

Topics: IoT Log and Sensor Data Analysis, Event Reconstruction, Anti-Forensic Techniques, Threats in Mobile and IoT Systems, Chain of Custody, Forensic Report Writing and Case Management.

Applications: Incident reconstruction, anomaly detection, secure forensic investigation, preparation of legal reports and documentation.

AI Integration: Machine learning for anomaly detection, automated report generation, visualization tools for forensic data analysis. **Authentic Intelligence:** Ethical considerations, legal accountability, risks of evidence tampering, importance of accurate and professional reporting.
NVIDIA DLI Free Courses (Relevant to this Module): **1. Accelerate Data Science Workflows with Zero Code Changes** (1 hr) | Path: Data Science Training – Data Preparation for Model Training https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+T-DS-03+V1

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Recall the basic concepts of Digital, Mobile and IoT Forensics, terminology, and forensic investigation steps.	L1
2	Describe the fundamental concepts of mobile and IoT forensics and understand device architectures and data storage.	L2
3	Apply mobile forensic acquisition techniques to extract and preserve digital evidence from devices.	L3
4	Analyze mobile and IoT data including cloud evidence to reconstruct events and user activities.	L4
5	Evaluate digital evidence, identify security threats, and prepare forensic reports following legal and ethical standards	L5

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs													
COs	**Program Outcomes (POs)**											**PSOs**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**1**	**2**
CO1	**1**	**1**		**-**	**-**	**-**	**-**	**-**	**-**	**-**	**1**	**1**	**1**
CO2	**2**	**2**	**1**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**1**	**2**	**2**
CO3	**3**	**2**	**2**	**1**	**2**	**1**	**1**	**-**	**2**	**1**	**1**	**2**	**2**
CO4	**3**	**3**	**2**	**2**	**2**	**2**	**1**	**-**	**2**	**1**	**1**	**2**	**2**
CO5	**3**	**3**	**3**	**2**	**2**	**2**	**2**	**1**	**2**	**1**	**2**	**2**	**2**

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Mobile Forensic Investigations – Lee Reiber, McGraw-Hill, 1st Edition.
2. Practical Mobile Forensics – Heather Mahalik, Packt Publishing, 3rd Edition.

REFERENCE BOOKS:

1. Digital Forensics – Eoghan Casey, Academic Press, 3rd Edition.
2. IoT Forensics: Challenges, Approaches and Applications – Shancang Li & Li Da Xu, Springer, 1st Edition.

RECOMMENDED TOOLS

- Forensic Tools: Cellebrite UFED, Oxygen Forensic Detective, Autopsy, FTK Imager
- Network Analysis: Wireshark, tcpdump
- IoT Analysis: Firmware Analysis Toolkit (FAT), Binwalk
- Programming: Python (for scripting and automation) – Google Colab / Jupyter Notebook / Visual Studio
- Visualization: Kibana, Grafana
- Investigation Platforms: Magnet AXIOM, EnCase
- AI Assistants: GitHub Copilot, ChatGPT, Claude

Operating System Security

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VII

Course Code	:		**Credits**		:	03
Hours / Week	:	03	**Total Hours**		:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**		:	60+40 Marks

Course Vision:

Examine prior research that defines the requirements of a secure operating system and explores implemented systems that effectively enforce security, in order to better understand how to balance functionality and security of the operating system.

Course Objectives:

This course will enable students:

1. Outline the models of protection and techniques to enforce security in operating systems.
2. Describe the impact of security features and access control mechanisms used in secure operating systems.
3. Summarizes a variety of ways that commercial operating systems have been extended with security features by using case studies.
4. Apply OS security principles in practical scenarios.
5. Explore virtualization and advanced OS security techniques.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with traditional lecture method, different types of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.

6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I Operating System Resource Security and Protection	**09 Hours**

Access and Flow Control – Introduction, Preliminaries, The access Matrix Model, Implementation of Access Matrix, Safety in the Access Matrix Model, Advanced Models of Protection, Case Studies: The UNIX operating System, The Hydra Kernel, Amoeba

Applications: File permissions and user access control in systems like UNIX operating system. Process isolation and memory protection. Role-Based Access Control (RBAC) for managing user privileges. Preventing unauthorized data access.

AI Integration: AI models learn normal access patterns and detect unusual behavior (e.g., insider threats). AI can adjust permissions in real time based on context (location, time, device). Machine learning can generate and optimize access control rules from usage data.

Authentic Intelligence: Critical decisions (like privilege escalation) require human approval alongside AI suggestions. Humans verify AI-generated access policies to avoid over-restriction or vulnerabilities

MODULE – II Access Control Fundamentals	**09 Hours**
Secure Operating Systems, Security Goals, Trust Model, Threat Model, Protection System, Lampson's Access Matrix, Mandatory Protection Systems, Reference Monitor, Secure Operating System Definition, Assessment Criteria, Multics History, The Multics System, Multics Security, Multics Vulnerability Analysis. Applications: Access control frameworks used in enterprise systems and cloud platforms like Microsoft Azure. Role-Based and Attribute-Based Access Control (RBAC/ABAC). Secure OS principles guide sandboxing, privilege separation, and isolation. Reference monitor concept used in secure kernels and hypervisors **AI Integration:** Intelligent Threat Modelling. Adaptive Trust Models. Smart Reference Monitor **Authentic Intelligence:** Risk-Aware Decision Making. Ethical and Fair Access Control	
MODULE – III Security in Ordinary Operating Systems, Verifiable Security Goals, Security Kernels	**09 Hours**
System Histories, UNIX Security, Windows Security, Information Flow, Information Flow Secrecy Models, Information Flow Integrity Models, The Security Kernel, Secure communications processor, Gemini Secure operating system. Applications: Minimal trusted computing base (TCB) using security kernels. Used in high-assurance systems like Gemini Secure Operating System. Verifiable security goals applied in certified systems. Ensures correctness of security mechanisms in critical applications **AI Integration:** Intelligent Information Flow Monitoring. Automated Verification. AI identifies malware and suspicious processes in operating systems. **Authentic Intelligence:** Experts validate AI-based verification of security kernels and OS models. Maintains balance between usability and strict security.	
MODULE – IV Securing Commercial Operating Systems	**09 Hours**
Retrofitting Security into a Commercial OS, History of Retrofitting Commercial OS's, Commercial Era, Microkernel Era, UNIX Era, Case Study1: Solaris Trusted Extensions, Case Study2: Building a Secure Operating System for Linux. **Applications:** Enterprise Operating System Security. Retrofitting Security in Legacy Systems. Cloud and Virtualization Security. **AI Integration:** Intelligent Retrofitting Analysis. Automated Vulnerability Detection. Adaptive Security Controls. **Authentic Intelligence:** Security professionals validate AI recommendations before applying changes to critical systems. Humans ensure compliance and correctness of AI-generated policies.	
MODULE – V Secure Testing, Tools & Best Practices	**09 Hours**

Capability System Fundamentals, Capability Security, Challenges in Secure Capability Systems, Building Secure Capability Systems, Separation Kernels, VAX VMM Security Kernel, Security in Other Virtual Machine Systems.

Applications: Secure Resource Management (Capability Systems). Virtual Machine Security. High-Assurance Systems.

AI Integration: Intelligent Capability Management. VM Behaviour Analysis. Automated Security Policy Enforcement.

Authentic Intelligence: Explainable Virtualization Security. Risk-Aware System Management

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	**Identify** and explain operating system security preliminaries including access and flow control, the access matrix model used in UNIX Operating System, Hydra Kernel, and Amoeba Distributed Operating System.	L2
2	**Outline** the fundamentals of access control in secure operating systems, including security goals, trust and threat models, and protection mechanisms using Lampson's Access Matrix and the Reference Monitor in the Multics Operating System.	L2
3	**Utilize** protection mechanisms, information flow models, and security kernels in systems such as UNIX, Microsoft Windows, and the Gemini Secure Operating System for achieving verifiable security goals.	L3
4	**Apply** operating system security principles to analyze and evaluate methods for retrofitting security into commercial operating systems through case studies such as Solaris Trusted Extensions and secure implementations in Linux.	L3
5	**Make Use of** capability-based security principles and virtual machine protection mechanisms to analyse secure capability systems and security kernels in virtualized environments such as VAX VMM Security Kernel.	L3

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs		
COs	**Program Outcomes (POs)**	**PSOs**

	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	2	2	1	-	-	-	-	-	-	-	-	1	2
CO2	2	2	1	-	-	-	-	-	-	-	-	1	2
CO3	3	3	1	-	-	-	-	-	-	-	-	1	2
CO4	3	2	2	-	-	-	-	-	-	-	-	1	2
CO5	3	2	1	-	-	-	-	-	-	-	-	1	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Mukesh Singhal and Niranjan Shivaratri, Advanced Concepts in Operating Systems, McGraw-Hill, 2011
2. Trent Jaeger, Operating System Security, Morgan & Claypool Publishers, 2008.

REFERENCE BOOKS:

1. Michael J. Palmer, "Guide To Operating Systems Security", 1st Edition, Cengage Learning, 2004.
2. Gerard Blokdyk, "Security-focused operating system: Master the Art of Design Patterns", CreateSpace Independent Publishing Platform, 2017.

RECOMMENDED TOOLS: Python, Java, Flask, Django, SQLite, MySQL, Scikit-learn, pgmpy, File Handling APIs, Basic VM simulation tools / datasets

CYBER RISK ANALYTICS & MANAGEMENT

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VII

Course Code	:		**Credits**	:	03
Hours / Week	:	03	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

The rapid expansion of interconnected digital systems, cloud infrastructures, and intelligent technologies has significantly increased the complexity of cyber threats and organizational risk exposure. This course focuses on advanced cyber risk analytics, quantitative risk assessment, threat intelligence, and predictive security analysis using statistical, probabilistic, and AI-driven approaches. It aims to develop analytical and strategic capabilities for intelligent cyber risk management, data-driven decision-making, and resilient cybersecurity operations in modern enterprise environments.

Course Objectives:

This course will enable students:

1. Understand advanced cyber risk concepts, cyber threat intelligence, and enterprise risk analytics methodologies.
2. Apply statistical, probabilistic, and data-driven techniques for cyber risk analysis and prediction.
3. Analyze security data, attack patterns, and behavioral indicators using analytical and visualization techniques.
4. Evaluate predictive cyber risk models, intelligent monitoring systems, and risk-informed security strategies.
5. Integrate AI, machine learning, and advanced analytical frameworks for intelligent cyber risk management and decision support.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. Lecture-based teaching integrated with analytical problem-solving and interactive learning methods.
2. Brainstorming sessions, group discussions, and case-study analysis on real-world cyber incidents and threat intelligence reports.
3. Demonstrations using cybersecurity analytics platforms, SIEM tools, visualization systems, and threat monitoring frameworks.
4. Hands-on exposure to statistical analysis, machine learning models, and cyber risk prediction techniques using real security datasets.
5. Encouraging critical thinking through analytical exercises, risk modeling problems, and scenario-based cybersecurity assessments.
6. Comparative analysis of cyber risk frameworks, predictive models, and intelligent defense strategies for enterprise environments.
7. Mini-projects focused on cyber threat analytics, anomaly detection, and AI-assisted risk intelligence systems.

MODULE – I	**09 Hours**

Cyber Risk Analytics Foundations

Topics: Cyber risk analytics concepts and architecture, cyber threat intelligence lifecycle, cyber risk data sources, structured and unstructured security data, threat indicators and attack telemetry, cyber attack patterns, cyber kill chain analytics, MITRE ATT&CK framework, security data collection methodologies, cyber risk metrics and KPIs, exposure analysis, attack surface analytics, enterprise cyber risk visibility.

Applications: Security monitoring systems, enterprise cyber intelligence, attack surface management, cyber threat analysis.

AI Integration: Threat intelligence automation, attack pattern recognition, intelligent risk classification systems.

Authentic Intelligence: Interpretation of contextual cyber intelligence, validation of analytical findings, ethical handling of security data.

MODULE – II	**09 Hours**

Statistical and Probabilistic Cyber Risk Analysis

Topics: Probability concepts in cybersecurity, statistical methods for cyber risk analysis, probability distributions, Bayesian analysis, Markov models, stochastic processes, likelihood estimation, cyber risk quantification, risk scoring methodologies, attack probability modeling, quantitative vs qualitative analysis, uncertainty analysis, statistical anomaly detection, confidence intervals in risk prediction.

Applications: Intrusion probability analysis, cyber attack forecasting, security risk estimation, vulnerability prioritization.

AI Integration: Probabilistic threat prediction systems, AI-driven anomaly detection, intelligent risk scoring engines.

Authentic Intelligence: Avoiding false positives and analytical bias, responsible interpretation of probabilistic models, human validation of automated predictions.

MODULE – III	**09 Hours**

Cyber Threat Intelligence and Behavioural Analytics

Topics: Cyber threat intelligence (CTI) frameworks, tactical and strategic intelligence, Indicators of Compromise (IoCs), adversary profiling, attacker tactics and techniques, user and entity behavior analytics (UEBA), insider threat analytics, malware behavior analysis, phishing behavior patterns, log analytics, SIEM-based behavioral monitoring, cyber deception techniques, social engineering analysis.

Applications: Threat hunting, insider threat detection, malware intelligence systems, fraud analytics.

AI Integration: Behavioral analytics using machine learning, deep learning for malware detection, AI-assisted SIEM systems.

Authentic Intelligence: Human oversight in behavioral analytics, ethical use of monitoring systems, interpretation of adversarial behavior.

MODULE – IV	**09 Hours**

Predictive Cyber Risk Modeling and Visualization

Topics: Predictive analytics in cybersecurity, cyber risk forecasting models, machine learning techniques for cyber risk prediction, supervised and unsupervised learning approaches, clustering and classification in cybersecurity, attack trend analysis, security visualization techniques, cyber risk dashboards, graph-based attack modeling, network traffic analytics, visualization of threat intelligence data.

Applications: Predictive security systems, cyber risk dashboards, network anomaly monitoring, enterprise risk forecasting.

AI Integration: Machine learning for attack prediction, intelligent visualization systems, automated trend analysis.

Authentic Intelligence: Responsible interpretation of predictive models, explainability in AI-driven cybersecurity, balancing automation with expert judgment.

MODULE – V	**09 Hours**

Advanced Cyber Risk Management and Decision Intelligence

Topics: Risk-driven cybersecurity strategy, cyber resilience engineering, advanced incident analytics, digital forensics intelligence, governance and compliance analytics, cloud risk analytics, IoT and AI system risk analysis, adversarial AI and evasion attacks, ransomware analytics, supply chain cyber risk, cyber insurance analytics, zero trust risk assessment, cyber risk decision-support systems, future trends in intelligent cyber defense.

Applications: Enterprise cyber defense, cloud and IoT security analytics, ransomware defense systems, strategic cyber risk management.

AI Integration: AI-driven cyber defense orchestration, adaptive security systems, intelligent incident response platforms.

Authentic Intelligence: Ethical AI usage in cybersecurity, accountability in automated defense systems, responsible cyber risk governance.

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
CO1	Explain cyber risk analytics concepts, cyber threat intelligence, and security data analysis techniques.	**L2**
CO2	Apply statistical, probabilistic, and analytical methods for cyber risk assessment and prediction.	**L3**
CO3	Analyze cyber threat intelligence, behavioral analytics, and attack patterns using security datasets and monitoring systems.	**L4**
CO4	Evaluate predictive cyber risk models, security visualization techniques, and intelligent risk assessment frameworks.	**L4**
CO5	Assess advanced cyber risk management strategies and AI-driven decision-support systems for enterprise cybersecurity.	**L4**

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs													
COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	3	2	1	-	-	-	2	-	-	-	1	2	1
CO2	3	3	2	2	3	-	2	-	-	-	1	3	2
CO3	3	3	3	2	3	-	2	-	-	-	1	3	3
CO4	2	3	3	3	3	-	3	-	-	-	1	3	2
CO5	2	3	3	3	3	-	3	-	-	-	2	3	3

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Tony UcedaVelez & Marco M. Morana – *Cyber Risk Analytics*, Wiley
2. Charles P. Pfleeger – *Security in Computing*, Pearson
3. William Stallings – *Cryptography and Network Security*, Pearson
4. Douglas W. Hubbard & Richard Seiersen – *How to Measure Anything in Cybersecurity Risk*, Wiley

REFERENCE BOOKS:

1. Ross Anderson – *Security Engineering*, Wiley
2. Bruce Schneier – *Applied Cryptography*, Wiley
3. Michael Whitman & Herbert Mattord – *Principles of Information Security*

MINI PROJECT THEMES

Students will design a cyber risk model or analytics-based system:

- Cyber attack prediction system
- Network anomaly detection tool
- Risk assessment dashboard
- Phishing detection system

- Security monitoring system

Students should demonstrate:

- Risk analysis
- Data analytics
- Security implementation
- Result interpretation

RECOMMENDED TOOLS

- Python
- Wireshark
- Kali Linux
- Splunk
- ELK Stack
- NumPy
- Pandas
- Scikit-learn

AGENTIC AI SECURITY

[As per Choice Based Credit System (CBCS) Scheme]

SEMESTER – VII

Course Code	:		Credits	:	03
Hours / Week	:	03	Total Hours	:	45
L–T–P–J	:	3–0–0–0	CIE + SEE	:	60+40 Marks

Course Vision: To build foundational knowledge of AI agent architectures, their security vulnerabilities, and practical defences so that students can assess risks and apply basic security principles to agentic AI systems.

Course Objectives: This course will enable students:

- Understand what AI agents are, how they work, and what makes them different from traditional software.
- Identify common attacks on AI agents such as prompt injection, jailbreaks, and data poisoning.
- Apply basic security principles — least privilege, access control, and input validation — to agentic systems.
- Explore how AI agents can be tested for vulnerabilities using red-teaming tools and frameworks.
- Appreciate the ethical and governance responsibilities when building and deploying AI agents.

Teaching-Learning Process (General Instructions)

These are sample pedagogical methods teachers can adopt to develop course outcomes:

- Lecture Method: Core concepts explained with real-world examples and case studies.
- Interactive Teaching: Hands-on attack/defence demos; group discussion on AI security incidents.
- Video/Animation: NVIDIA DLI course videos and live tool demonstrations.
- Collaborative Learning: Pair labs for building and attacking simple agents.
- Hands-On Coding: NVIDIA DLI Jupyter notebooks using GPU-accelerated cloud environments.

MODULE – I- Introduction to AI Agents & Security Basics	09 Hours

Topics: What is an AI agent? Goals, tools, memory, and actions; Types of agents: chatbots, coding assistants, research agents, multi-agent systems; How does agentic AI differ from regular software in terms of security? Basic threat model: who attacks, what they want? How do they attack? Overview of OWASP Top 10 for Agentic AI and MITRE ATLAS framework

Applications: A customer service chatbot that can be tricked into leaking data; A coding assistant that runs unsafe commands if instructed to; A research agent that visits malicious web pages

AI Integration: Set up a simple LangChain agent with a tool; identify its inputs, outputs, and possible attack points; map them to OWASP Agentic AI categories using Jupyter on Google Colab.

Authentic Intelligence: Deep understanding of Agents

MODULE – II: Prompt Injection & Jailbreak Attacks	09 Hours

Topics: Prompt injection ;direct and indirect attacks; Jailbreaking: tricking an AI to ignore its safety rules; Real examples: injections via emails, web pages, tool outputs; How semantic firewalls and guardrails detect and block these attacks? Using NVIDIA NeMo Guardrails: topic control and jailbreak detection; Introduction to garak — a tool for scanning LLM vulnerabilities

Applications: Injecting instructions into a helpdesk agent via a customer email; Tricking a coding agent to run malicious code through crafted prompts; Bypassing a chatbot's safety rules using role-play jailbreaks

AI Integration: Attempt a direct prompt injection on a LangChain agent; run garak to scan for vulnerabilities; configure a NeMo Guardrails jailbreak-detect rail and test its effectiveness on Google Colab.

Authentic Intelligence: Conceptual understanding of guardrails and firewalls

MODULE – III- Access Control, Tool Security & Agent Identity	09 Hours

Topics: Why do agents need access control?least privilege and permission scoping; How agents use tools? risks of unrestricted tool access; OAuth 2.0 basics: giving agents only the permissions they need; Agent identity: how do we know which agent is taking an action?; Agent impersonation: when one agent pretends to be another; Introduction to Model Context Protocol (MCP) and its security risks

Applications: A coding agent with unrestricted file access deletes important files; An agent that impersonates an admin agent to gain higher privileges; A compromised MCP tool that injects malicious instructions

AI Integration: Build a tool-using LangGraph agent; add a scoped permission layer; simulate an impersonation attack between two agents and observe the impact; apply a simple validation defence on Google Colab.

Authentic Intelligence: Analysis of access control mechanisms and agent identity

MODULE – IV- Data Security & Adversarial Attacks on AI Agents	09 Hours

Topics: Training data poisoning: how bad data corrupts an AI agent's behaviour? RAG attacks: poisoning the documents an agent retrieves; Membership inference: guessing whether your data was used to train a model; How NeMo Guardrails detects and blocks sensitive data leakage (PII); Adversarial examples: small changes to inputs that fool AI models; Basic defences: input validation, output filtering, data sanitisation.

Applications: Poisoning a company knowledge base to make a customer agent give wrong answers; An agent leaking personal data when queried in a specific way; An adversarial image that fools an AI-powered security camera

AI Integration: Poison a small RAG vector store; observe how the agent's answers change; deploy a NeMo retrieval-grounding guardrail to fix it; test PII detection using NeMo Guardrails on Google Colab.

Authentic Intelligence: Evaluation of attacks in RAG

MODULE – V- Red Teaming, AI Safety & Responsible Use	09 Hours

Topics: What is AI red teaming? Finding weaknesses before attackers do; OWASP Top 10 for Agentic AI: the most important risks to test for; When AI agents go wrong? unexpected behaviours and how to detect them; Human-in-the-loop: keeping humans in control of high-stakes decisions; AI governance basics: NIST AI RMF and responsible AI principles; Ethical considerations: bias, misuse, and accountability in agentic AI

Applications: Red-teaming a simple chatbot agent using the OWASP Agentic AI checklist; An AI hiring agent that exhibits biased behaviour due to bad training data; Designing a human approval step for an agent that sends emails autonomously

AI Integration: Run a structured red-team test on a multi-tool agent using the OWASP ASI Top 10 checklist; document findings; propose fixes; discuss ethical implications using real case studies on Jupyter.

Authentic Intelligence: Evaluation of Red Teaming and AI Governance

Course Outcomes

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Explain what AI agents are, describe their components, and identify the basic security risks they introduce compared to traditional software.	L2
2	Recognise and describe common attacks on AI agents — prompt injection, jailbreaks, and data poisoning — and explain how guardrails can prevent them.	L2
3	Apply least-privilege access control and input validation principles to a simple agentic system and demonstrate how improper access leads to security failures.	L3
4	Set up and implement a basic red-team test on an AI agent using the OWASP Agentic AI Top 10 checklist and document identified vulnerabilities.	L4
5	Analyze the ethical responsibilities, governance frameworks (NIST AI RMF), and responsible deployment practices relevant to AI agentic systems.	L4

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	1	2	3	4	5	6	7	8	9	10	11	PSO 1	PSO 2
CO1	3	2	1	-	-	2	-	-	2	-	1	2	2
CO2	3	2	1	1	1	2	1	-	2	1	1	2	2
CO3	3	3	2	2	1	2	1	1	2	1	1	2	2
CO4	3	3	2	2	2	2	1	1	2	1	1	2	2
CO5	2	2	1	1	2	3	2	1	3	1	2	2	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. OWASP GenAI Security Project. (2026). OWASP Top 10 for Agentic Applications 2026. genai.owasp.org.
2. OWASP GenAI Security Project. (2025). Securing Agentic Applications Guide v1.0. genai.owasp.org.
3. Huang, K. (Ed.). (2025). Agentic AI. Progress in IS. Springer, Cham.
4. NIST. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1.
5. Vorobeychik, Y., & Kantarcioglu, M. (2018). Adversarial Machine Learning. Morgan & Claypool Publishers. (Selected chapters)

REFERENCE BOOKS:

1. Bertino, E. (2026). CS 59200: AI Agentic Security — Seminar Syllabus. Purdue University.
2. OWASP AI Exchange. (2025). AI Security Threats, Controls and Best Practices. owaspai.org.
3. NVIDIA. (2025). Safety and Security Framework for Real-World Agentic Systems. developer.nvidia.com.
4. Google. (2025). Secure AI Framework (SAIF) 2.0: Focus on Agents.
5. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press. deeplearningbook.org.

RECOMMENDED TOOLS & FRAMEWORKS

1. NVIDIA NeMo Guardrails — jailbreak detection, topic control, PII detection for agentic pipelines (developer.nvidia.com/nemo-guardrails)
2. garak — LLM red-teaming and vulnerability scanner
3. LangChain / LangGraph — agent building and security labs
4. IBM Adversarial Robustness Toolbox (ART) — adversarial attack and defence implementation
5. OWASP ASI Top 10 (2026) — agentic AI security checklist and red-team framework
6. MITRE ATLAS — adversarial threat landscape for AI systems
7. Programming: Python 3 (PyTorch, scikit-learn) — Google Colab / Jupyter (NVIDIA GPU-enabled)

OPEN ENDED LAB EXERCISES

S.No	Exercise Title	Aim / Objective	Tools	Hrs	CO
MODULE I · Exercises 1–3 : AI Agents & Security Basics (06 Hours)					
1	Build a Simple Agent	Create a LangChain agent with one tool (web search); identify its inputs, outputs, and potential attack points.	Google Colab / LangChain / Python	2 h	CO1

2	OWASP Agentic AI Mapping	Map the components of your agent to the OWASP Top 10 for Agentic AI categories; discuss which risks apply and why.	Jupyter / OWASP ASI checklist	2 h	CO1
3	Threat Modelling Exercise	Use MITRE ATLAS to identify three realistic attack scenarios for a simple customer service agent and document mitigations.	MITRE ATLAS / Jupyter	2 h	CO1
MODULE II · Exercises 4–6 : Prompt Injection & Jailbreaks (06 Hours)					
4	Direct Prompt Injection	Craft and test direct prompt injection attacks on a LangChain agent; measure how often the attack succeeds.	Google Colab / LangChain / Python	2 h	CO2
5	LLM Vulnerability Scan with garak	Run garak on a hosted LLM to scan for jailbreak and injection vulnerabilities; summarise findings in a short report.	Google Colab / garak	2 h	CO2
6	Deploy NeMo Guardrails	Configure a NeMo Guardrails jailbreak-detect rail on an agent; compare attack success rate before and after.	Google Colab / NeMo Guardrails	2 h	CO2
MODULE III · Exercises 7–9 : Access Control & Identity (06 Hours)					
7	Tool Permission Scoping	Build a two-tool agent; demonstrate that unrestricted access causes damage; add permission scoping and verify the fix.	Google Colab / LangGraph / Python	2 h	CO3
8	Agent Impersonation Attack	Simulate a simple agent impersonation in a two-agent setup; implement a validation check to detect and block it.	Google Colab / CrewAI / Python	2 h	CO3
9	MCP Security Review	Examine a sample MCP server configuration; identify one tool-squatting and one schema-manipulation risk; propose fixes.	Google Colab / MCP SDK / Python	2 h	CO3
MODULE IV · Exercises 10–12 : Data Security & Adversarial Attacks (06 Hours)					

10	RAG Poisoning Attack	Poison a small vector store with a malicious document; observe the agent's changed behaviour; apply a guardrail to fix it.	Google Colab / LlamaIndex / NeMo Guardrails	2 h	CO4
11	FGSM Adversarial Example	Generate an FGSM adversarial image using IBM ART; test it against an image classifier; visualise the perturbation.	Google Colab / IBM ART / PyTorch	2 h	CO4
12	PII Detection with NeMo Guardrails	Configure a NeMo PII-detection rail; test it by querying an agent with prompts designed to leak personal data.	Google Colab / NeMo Guardrails / Python	2 h	CO4
MODULE V · Exercises 13–15 : Red Teaming & Responsible AI (06 Hours)					
13	OWASP ASI Red-Team Checklist	Run through the OWASP Top 10 for Agentic AI against a multi-tool agent; record which risks are present and their severity.	Google Colab / OWASP ASI / LangGraph	2 h	CO5
14	Add Human-in-the-Loop Control	Modify an agent that sends emails autonomously to require human approval for sensitive actions; test the safeguard.	Google Colab / LangGraph / Python	2 h	CO5
15	AI Ethics Case Study	Analyse a real agentic AI failure case; apply NIST AI RMF categories; write a one-page responsible-use recommendation.	Jupyter / NIST AI RMF	2 h	CO5

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

CRYPTOGRAPHY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VII

Course Code	:		**Credits**	:	03
Hours / Week	:	03	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

To create awareness of cryptographic techniques and enable students to understand and apply fundamental concepts for securing digital information and communication in real-world systems.

Course Objectives:

This course will enable students to:

1. Introduce basic concepts of cryptography and its role in information security.
2. Explain fundamental encryption techniques used in modern digital systems.
3. Illustrate applications of cryptographic methods in real-world scenarios.
4. Develop understanding of authentication, data integrity, and secure communication.
5. Create awareness about common security threats and protection mechanisms.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with presentation-based teaching to explain cryptographic concepts.
2. **Interactive Teaching:** brainstorming, discussions, and case studies on real-world security scenarios.
3. **Showing video/animation films** to demonstrate encryption, hashing, and secure communication.
4. **Encourage Collaborative (Group Learning) learning** through mini-projects and problem-solving.
5. To **develop critical thinking, asking higher order thinking questions** through quizzes and case-based analysis.
6. **Demonstrating multiple approaches** to solve security problems and encouraging innovative solutions.

MODULE – I: Fundamentals of Cryptography	**10 Hours**

Security goals and terminology, Classical cryptography: Caesar cipher, substitution cipher, transposition cipher, cryptanalysis techniques, limitations of classical cryptography, need for modern cryptography, overview of cryptography in real-world systems.

Applications: Secure messaging systems, Password protection, Data privacy in online platforms

AI Integration: Data privacy in AI applications, Secure handling of user data

Authentic Intelligence: Risks of weak security practices, Awareness of data protection

MODULE – II: Symmetric Key Cryptography	**08 Hours**

Concept of symmetric key encryption, block ciphers, Data Encryption Standard (DES), Advanced Encryption Standard (AES), modes of operation. Applications in real-world systems.

Applications: File and disk encryption, Wi-Fi security, Data protection in devices

AI Integration: Protecting AI datasets, Secure storage of model data

Authentic Intelligence: Choosing secure encryption methods, Avoiding weak configurations

MODULE – III: Public Key Cryptography	**09 Hours**

Asymmetric cryptography, public and private keys, RSA algorithm, Diffie-Hellman key exchange, digital certificates, secure communication mechanisms.

Applications: Secure web browsing, Online banking, Secure communication systems

AI Integration: Secure communication in distributed AI, Cloud-based AI security

Authentic Intelligence: Trust in digital communication, Ethical use of cryptographic systems	
MODULE – IV: Hashing & Digital Signatures	**09 Hours**
Cryptographic hash functions, SHA-256, password hashing, Message Authentication Codes (MAC), digital signatures, authentication and authorization concepts. **Applications:** Secure login systems, Data integrity verification, Digital document authentication **AI Integration:** Data integrity in AI pipelines, Secure authentication in AI systems **Authentic Intelligence:** Preventing data tampering, Responsible authentication practices	
MODULE – V: Cryptography in Practice & Security Attacks	**09 Hours**
SSL/TLS, HTTPS, cryptography in blockchain and cloud systems, phishing attacks, replay attacks, Man-in-the-Middle attacks, case studies of data breaches and weak security practices. **Applications:** Secure web communication (HTTPS), Cloud security, Cybersecurity awareness **AI Integration:** AI-based threat detection, Secure AI communication **Authentic Intelligence:** Awareness of cyber threats, Responsible digital behavior	

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Explain cryptographic fundamentals, classical encryption techniques, and security goals for protecting digital information	L2
2	Apply symmetric key cryptographic techniques and block cipher mechanisms for securing data and communication systems	L3
3	Apply public key cryptography, key exchange mechanisms, and digital certificates for secure communication	L3
4	Analyze hashing techniques, authentication mechanisms, and digital signatures for ensuring data integrity and authentication	L4
5	Evaluate cryptographic applications, security threats, and protection mechanisms in modern communication and cloud-based systems	L5

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs													
COs	**Program Outcomes (POs)**											**PSOs**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**1**	**2**
CO1	3	2	-	-	-	-	1	-	-	-	1	2	2
CO2	3	2	2	-	2	-	1	-	-	-	1	3	2
CO3	3	3	2	1	2	-	1	-	-	-	1	3	3
CO4	3	3	2	2	2	-	1	-	-	-	1	3	3
CO5	2	3	2	2	2	1	2	-	-	-	2	2	3

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. William Stallings, *Cryptography and Network Security: Principles and Practice*, Seventh Edition, Pearson Education, 2017.
2. Behrouz A. Forouzan, *Cryptography and Network Security*, Third Edition, McGraw-Hill Education, 2015.

REFERENCE BOOKS:

1. Jonathan Katz, Yehuda Lindell, *Introduction to Modern Cryptography*, Third Edition, CRC Press, 2020.
2. Christof Paar, Jan Pelzl, *Understanding Cryptography*, Springer, 2010.
3. Bruce Schneier, *Applied Cryptography*, Second Edition, Wiley, 2015.

RECOMMENDED TOOLS

- Python
- PyCryptodome
- OpenSSL
- Wireshark
- Jupyter Notebook

DIGITAL FORENSICS

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VII

Course Code	:		**Credits**	:	03
Hours / Week	:	03	**Total Hours**	:	45
L-T-P-J	:	3-0-0-0	**CIE+SEE**	:	60+40 Marks

Eligible Branches: Civil Engineering | Mechanical Engineering | Electrical & Electronics Engineering | Electronics & Communication Engineering | Information Science Engineering | Biotechnology | Aerospace Engineering | Industrial Engineering | All other B.E. / B.Tech programs

Prerequisite: Basic Computer Operation & Internet Usage. No prior programming or cybersecurity knowledge required.

Course Vision: To develop awareness, investigative thinking, and practical skills in digital forensics among engineering students of all disciplines — enabling them to identify, preserve, and analyze digital evidence from

computers, mobile devices, and networks, and apply forensic principles responsibly in their professional and academic domains.

Course Objectives: This course will enable students:

1. To understand the digital forensics lifecycle, legal framework, and ethical responsibilities in investigating digital evidence across engineering and professional environments.
2. To identify and analyze digital evidence from computers, storage devices, and file systems using accessible forensic tools without requiring programming expertise.
3. To investigate digital artifacts from email, social media, mobile devices, and IoT systems relevant to engineering industries.
4. To understand network-based evidence, cybercrime investigation techniques, and the role of digital forensics in industrial control systems and critical infrastructure.
5. To document forensic findings, produce professional investigation reports, and apply digital forensic awareness in engineering project and workplace contexts.

Teaching-Learning Process (General Instructions)

These are sample pedagogical methods where the teacher can use to accelerate the attainment of the various course outcomes. Since this is an open elective for all engineering branches, methods are designed to be inclusive and accessible without programming prerequisites:

1. **Lecture method** along with traditional lecture method, different types of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them.

MODULE - I : Introduction to Digital Forensics	**09 Hours**

Topics:

What is Digital Forensics: Definition, scope, goals, and importance in the digital age; Difference between digital forensics, cybersecurity, and cyber law; Categories of digital evidence: structured, unstructured, and volatile data. Digital Forensics Lifecycle: Identification, preservation, collection, examination, analysis, and presentation of evidence. Legal & Ethical Framework: Indian IT Act 2000 and its amendments; Evidence Act provisions for electronic records; Chain of custody: definition, importance, and documentation; Admissibility of digital evidence in Indian courts.

AI Integration:

Discussion of how AI is changing the landscape of digital evidence in engineering contexts; Introduction to using AI assistants (ChatGPT, Claude) for legal research and forensic report drafting.

Authentic Intelligence:

Understanding the boundaries between forensic investigation and invasion of privacy; Ethical obligations when discovering colleague misconduct through digital evidence;.

NVIDIA DLI Free Courses (Relevant to this Module):

1. **Introduction to Cybersecurity** (6 hrs) | Path: Cybersecurity Training - Fundamentals | https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-CS-01+V1

MODULE - II : Computer & Storage Media Forensics	**09 Hours**

Topics:

Computer Hardware Basics for Forensics: Storage devices: HDD, SSD, USB drives, SD cards, optical media; How data is stored and why deleted files are recoverable; Disk partitions, file systems, and data organization (FAT32, NTFS, ext4) - conceptual overview without programming. File System Forensics (Tool-Based): Understanding file metadata: created, modified, accessed timestamps (MAC times); Hidden files, file extensions, and disguised file types; Deleted file recovery concepts: unallocated space and file carving; Slack space and steganography: hiding data inside innocent-looking files. Practical Forensic Imaging: What is a forensic image and why is it needed; Write blockers: purpose and usage; Introduction to forensic imaging tools: FTK Imager (GUI-based), Recuva; Hash verification: MD5 and SHA-256 for evidence integrity

AI Integration:

Using AI-assisted tools (Autopsy plugins) for automated file classification and metadata extraction.

Authentic Intelligence:

Privacy implications of full-disk forensic imaging in engineering workplace investigations.

MODULE - III : Email, Social Media, & Mobile Forensics	**09 Hours**

Topics:

Email Forensics: Structure of an email: headers, body, attachments; Tracing email origin using email header analysis (GUI tools); Email spoofing and phishing identification; Recovering deleted emails from mail clients and web-based services; Email evidence in harassment, fraud, and intellectual property cases. Social Media Forensics: Digital footprint: what data social media platforms retain; Open Source Intelligence (OSINT): ethically gathering public information. Mobile Device Forensics: Smartphone data categories: call logs, SMS, contacts, app data, GPS history, photos; Types of mobile forensic acquisition: manual, logical, and physical (conceptual); Tools: MSAB XRY (overview), Cellebrite (overview), Android/iOS data extraction using Oxygen Forensics; Mobile evidence in accident reconstruction and workplace incident investigations.

AI Integration:

Machine learning-based phishing email detection from header and content patterns; AI-assisted mobile data analysis.

Authentic Intelligence:

Legal boundaries of collecting social media evidence without a court order; Ethical risks of OSINT: the line between public information gathering and stalking.

MODULE - IV : Network Forensics & Cybercrime Investigation	**09 Hours**

Topics:

Network Forensics Basics: What is network traffic and why it matters for investigations; IP addresses, MAC addresses, and how devices are identified on a network; Introduction to packet capture: what Wireshark shows (GUI walkthrough - no coding required); Log files as forensic evidence: web server logs, firewall logs, router logs; Identifying suspicious network activity: unauthorized access, data exfiltration, DDoS patterns. Cybercrime Investigation Techniques: Incident response lifecycle: detect, contain, eradicate, recover, document; Types of malware and their behavior: viruses, ransomware, spyware, trojans; Ransomware attack investigation: timeline reconstruction and evidence collection; Social engineering and phishing investigation workflow; Dark Web Awareness: What the dark web is and its relevance to cybercrime investigations; How stolen engineering data and intellectual property appears on dark web markets; Responsible awareness without participation.

AI Integration:

AI-based network traffic anomaly detection.

Authentic Intelligence:

Ethical obligations when discovering a cyberattack in progress within an organization.

MODULE - V : Forensic Reporting & Ethics	**09 Hours**

Topics:

Forensic Investigation Reporting: Structure of a professional digital forensic investigation report: executive summary, methodology, findings, conclusions, recommendations; Chain of custody documentation: forms, logs, and evidence bags; How to present technical findings to non-technical stakeholders (management, legal teams, courts); Common mistakes in forensic reports and their legal consequences. Anti-Forensics Awareness: What anti-forensics means: file wiping, encryption, steganography, log deletion; Why anti-forensics matters for investigators: knowing what evidence may have been destroyed; Introduction to detection approaches (tool-level, not programming-level). Ethical and Professional Responsibilities: Professional ethics for engineers encountering digital evidence; Whistleblower protection and legal obligations for reporting cybercrime discovered at work; Intellectual property protection for engineers: safeguarding project files, designs, and research data.

AI Integration:

AI and deepfake detection tools; Automated forensic report generation using AI writing assistants.

Authentic Intelligence:

Transparency obligations when AI tools are used to generate or support forensic findings.

Course Outcomes		
Course Outcomes (COs)	**Description**	**Bloom's Taxonomy Level**
At the end of the course the student will be able to:		
1	Explain the digital forensics lifecycle, legal framework, chain of custody principles, and ethical responsibilities associated with handling digital evidence in engineering and professional environments.	**L2**
2	Identify and recover digital artifacts from computers, storage media, and file systems using GUI-based forensic tools, and document findings with proper evidence integrity verification.	**L3**
3	Investigate digital evidence from email, social media, and mobile devices, relevant to engineering industry incident scenarios.	**L3**
4	Analyze network logs and cybercrime incident patterns to reconstruct attack timelines and support incident response in engineering environments.	**L4**
5	**Explain** the process of forensic report writing, **identify** common anti-forensic techniques	**L2**

Table: Mapping Levels of COs to POs / PSOs

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	2	2	1	-	1	2	1	1	-	-	1	2	2
CO2	2	2	1	1	1	1	1	-	-	-	1	2	2
CO3	2	2	1	1	1	2	1	1	1	1	1	2	2
CO4	3	2	2	1	1	2	1	1	2	1	1	2	2
CO5	3	2	2	1	1	2	1	1	2	1	1	2	2

3: Substantial (High) 2: Moderate (Medium) 1: Poor (Low)

TEXT BOOKS:

1. Digital Forensics and Incident Response - Gerard Johansen, Packt Publishing, 2nd Edition, 2020.
2. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics - John Sammons, Syngress (Elsevier), 2nd Edition, 2014.

REFERENCE BOOKS:

1. Cybercrime and Digital Forensics: An Introduction - Thomas J. Holt, Adam M. Bossler & Kathryn C. Seigfried-Spellar, Routledge, 3rd Edition, 2022.
2. Digital Evidence and Computer Crime - Eoghan Casey, Academic Press (Elsevier), 3rd Edition, 2011.
3. Guide to Computer Forensics and Investigations - Bill Nelson, Amelia Phillips & Christopher Steuart, Cengage Learning, 6th Edition, 2019.

RECOMMENDED TOOLS (GUI-Based - No Programming Required):

Forensic Imaging: FTK Imager (free GUI tool), Recuva (deleted file recovery), Autopsy (open-source GUI forensic platform)
Mobile Forensics: Oxygen Forensic Detective (educational trial), Android Backup Extractor, iExplorer (iOS)
Network Analysis: Wireshark (GUI packet capture and analysis), NetworkMiner (GUI-based network forensics)
Report Writing Aids: Autopsy report export, Forensic case report templates, Microsoft Word / Google Docs
AI Assistants: ChatGPT, Claude, Copilot (for report drafting, legal research, and case summarization)

SCHOOL OF ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

AI IN AUTOMOTIVE SECURITY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – VIII

Subject Code :	**Credits** : 03
Hours / Week :3	**Total Hours** : 45
L–T–P–S :3-0-0-0	

Course Learning Objectives:

This course will enable students to:

1. To summarize the fundamentals of automotive systems, connected vehicles, and AI-enabled automotive architectures.
2. To understand automotive communication networks, cybersecurity threats, and vulnerabilities in intelligent transportation systems.
3. To apply AI techniques, security mechanisms, and cryptographic methods for automotive system protection.
4. To analyze automotive cybersecurity standards, risk assessment methodologies, and secure development practices.
5. To evaluate emerging trends, future challenges, and AI-driven security solutions in autonomous and connected vehicles.

1. **Teaching-Learning Process (General Instructions)**
2. These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.
3. 1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
4. 2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
5. 3. Show ***Video/animation*** films to explain the functioning of various concepts.
6. 4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
7. 5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
8. 6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	**09 Hours**

Introduction to Automotive Cyber Security with AI Foundations

Topics: Introduction to Automotive Cyber Security, Evolution of Connected and Autonomous Vehicles, Intelligent Transportation Systems (ITS), Electronic Control Units (ECUs), Smart Sensors and Actuators, In-Vehicle Communication Networks, CAN, LIN, FlexRay, Automotive Ethernet, Vehicle-to-Everything (V2X) Communication, Automotive Software Architectures, Cybersecurity Principles in Automotive Systems, Confidentiality, Integrity and Availability (CIA), AI Foundations for Automotive Systems, Machine Learning in Autonomous Driving, Data Acquisition and Sensor Fusion.

Applications: Connected vehicles, autonomous driving systems, intelligent transportation, smart vehicle monitoring.

AI Integration: Introduction to AI-driven automotive systems, perception models, intelligent sensor analytics, and machine learning for vehicle control.

Authentic Intelligence: Challenges in securing connected vehicles, risks from AI model manipulation, limitations in autonomous decision-making systems.

UNIT – II	09 Hours

AI-Driven Automotive Threats, Vulnerabilities and Attack Techniques

Topics:Threat Modeling in Automotive Systems, Vulnerability Analysis, Attack Surface Identification, CAN Injection Attacks, Replay Attacks, Spoofing Attacks, Malware in Automotive Systems, Adversarial Machine Learning, Data Poisoning Attacks, Model Evasion Techniques, Adversarial Examples in Autonomous Vehicles, Sensor Manipulation Attacks, GPS Spoofing, Firmware Exploitation, Automotive Penetration Testing, Case Studies of Automotive Cyber Attacks, AI-Specific Threats in Autonomous Systems.

Applications: Threat analysis for connected vehicles, automotive penetration testing, autonomous vehicle security evaluation.

AI Integration: Machine learning models for attack detection, AI-assisted vulnerability assessment, anomaly detection in vehicle communication.

Authentic Intelligence: Challenges in detecting sophisticated attacks, risks of adversarial AI, security weaknesses in autonomous driving models.

UNIT – III	09 Hours

AI-Enhanced Automotive Security Mechanisms and Cryptography

Topics: Automotive Security Architectures, Encryption Techniques, Authentication Mechanisms, Secure Onboard Communication (SecOC), Hardware Security Modules (HSM), Public Key Infrastructure (PKI), Secure Boot, Intrusion Detection Systems (IDS), AI-Based Intrusion Detection, Deep Learning for CAN Traffic Analysis, Federated Learning for Vehicle Security, Privacy-Preserving AI, Secure OTA Updates, Middleware and APIs for Automotive Systems, Distributed Automotive Platforms, Cloud and Edge Computing in Vehicles.

Applications:

Secure connected vehicles, intelligent intrusion detection, secure automotive communication systems.

AI Integration:

AI-driven anomaly detection, intelligent authentication systems, adaptive security policies using machine learning.

Authentic Intelligence:

Latency issues in real-time security, scalability challenges in vehicle networks, privacy concerns in automotive AI systems.

UNIT – IV	09 Hours

Standards, Regulations, and AI-Secure Development Practices

Topics:

Automotive Cybersecurity Standards, ISO/SAE 21434, UNECE WP.29, Threat Analysis and Risk Assessment (TARA), AI-Aware Threat Modeling, Secure Software Development Lifecycle (SSDLC), AI Model Lifecycle Security, Security Validation Techniques, Automotive Fuzz Testing, Reinforcement Learning for Security Testing, Compliance Verification, Risk Management Techniques, Functional Safety and Security Integration, Explainable AI (XAI) in Automotive Systems, Secure System Design Principles.

Applications:

Secure automotive software development, compliance verification, intelligent automotive risk assessment.

AI Integration:

AI-assisted penetration testing, intelligent compliance analysis, reinforcement learning for automotive security validation.

Authentic Intelligence:

Bias and reliability issues in AI models, challenges in secure AI deployment, complexity of automotive compliance requirements.

UNIT – V	09 Hours

AI in Emerging Trends and Future Automotive Cyber Security

Topics:

Autonomous Vehicle Security, AI-Powered Threat Intelligence, Secure Vehicle-to-Everything (V2X) Communication, Blockchain in Automotive Security, Post-Quantum Cryptography, Self-Healing Vehicle Systems, Explainable AI for Automotive Cybersecurity, Predictive Threat Analytics, Intelligent OTA Security, Cyber Threat Intelligence (CTI), Edge AI Security, Secure Smart Mobility Systems, Ethical Issues in Autonomous Transportation, Future Research Challenges in Automotive Cybersecurity.

Applications:

Secure autonomous transportation, intelligent mobility systems, next-generation connected vehicle ecosystems.

AI Integration:

AI-based predictive security analysis, intelligent monitoring systems, automated cyber threat response mechanisms.

Authentic Intelligence:

Security vulnerabilities in autonomous systems, ethical concerns in AI-driven vehicles, challenges in large-scale deployment of intelligent transportation systems.

Course Outcomes:

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

1. Explain automotive system architecture and identify potential attack surfaces in connected vehicles.
2. Analyze and evaluate cybersecurity threats and vulnerabilities in automotive networks.
3. Apply appropriate security mechanisms and cryptographic techniques to protect automotive systems.
4. Interpret and implement automotive cybersecurity standards such as ISO/SAE 21434 in system design.
5. Assess emerging technologies and propose solutions for securing next-generation automotive systems.

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
CO1	Recall basic concepts of automotive systems and AI-enabled connected vehicles.	L1
CO2	Describe automotive architectures, communication protocols, and cybersecurity threats.	L2
CO3	Apply AI techniques, cryptographic methods, and security mechanisms for automotive protection.	L3
CO4	Analyze automotive risks, standards, and secure development methodologies.	L4
CO5	Evaluate emerging technologies and future security challenges in autonomous and connected vehicles.	L5

Mapping Levels of COs to POs / PSOs

	POs											PSOs	
COs	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**1**	**2**
CO1	1	1	-	-	-	-	-	-	-	-	1	1	1
CO2	2	2	1	-	-	-	-	-	-	-	1	2	2
CO3	3	2	1	1	1	2	1	-	2	1	1	2	2
CO4	3	2	1	1	1	2	1	-	2	1	1	2	2
CO5	3	2	1	1	1	2	1	-	2	1	1	2	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Automotive Cybersecurity Engineering Handbook – Marko Wolf & André Weimerskirch, Packt Publishing, 1st Edition.
2. The Car Hacker's Handbook – Craig Smith, No Starch Press, 1st Edition.

REFERENCE BOOKS:

1. Automotive Cyber Security: Introduction, Challenges, and Standardization – Shiho Kim & Rakesh Shrestha, Springer.
2. Guide to Automotive Connectivity and Cybersecurity – Dietmar P.F. Möller & Roland E. Haas, Springer.
3. Automotive Cybersecurity: An Introduction to ISO/SAE 21434 – David Ward & Paul Wooderson, SAE International.
4. Automotive Cybersecurity Engineering Handbook – Ahmad MK Nasser, Packt Publishing.

RECOMMENDED TOOLS

Programming:
Python (NumPy, Pandas, TensorFlow, PyTorch) – Google Colab / Jupyter Notebook

Automotive Security Tools:
CANoe, CANalyzer, Wireshark, Scapy

Simulation Platforms:
MATLAB/Simulink, CARLA Simulator

Cloud Platforms:
AWS IoT, Azure IoT Hub

Visualization:
Grafana, Power BI, Tableau

AI Assistants:

GitHub Copilot, ChatGPT, Claude

ADVANCED FORENSICS AND LEGAL EXPERTISE

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VIII

Course Code	:		**Credits**	:	03
Hours / Week	:	03	**Total Hours**	:	45

L–T–P–J	**:**	3–0–0–0	**CIE + SEE**	**:**	60 + 40 Marks

Course Vision: To develop highly skilled forensic practitioners who integrate advanced investigative techniques with deep legal expertise, enabling them to collect, preserve, analyze, and present digital evidence with scientific rigor, legal precision, and ethical integrity across diverse judicial and organizational contexts.

Course Objectives: This course will enable students:

- To understand advanced forensic investigation frameworks, expert witness standards, and the legal ecosystem governing digital evidence.
- To master advanced disk, file system, memory, and artifact-level forensic techniques using industry-standard and open-source tools.
- To conduct advanced network, cloud, and enterprise forensic investigations including multi-source log correlation and cross-jurisdictional evidence handling.
- To apply advanced mobile, IoT, and embedded device forensic techniques across diverse physical, logical, and cloud extraction methods.
- To develop expertise in malware analysis, reverse engineering, legal report writing, and courtroom expert testimony aligned with Indian and international cyber law.

Teaching-Learning Process (General Instructions)

These are sample pedagogical methods for attaining course outcomes:

- Lecture Method: case-driven walkthroughs of real-world forensic investigations, landmark cybercrime court cases, and legal precedents.
- Interactive Teaching: moot court simulations, expert witness testimony drills, and evidence admissibility debates.
- Hands-on Lab Sessions using forensic tools such as Autopsy, FTK Imager, Volatility, Wireshark, Cellebrite UFED, and Ghidra.
- Video/Animation: walkthroughs of forensic tool usage, courtroom expert testimony recordings, and cyber law case studies.
- Collaborative Learning: team-based forensic case analysis, drafting court-ready reports, and peer review of investigation findings.
- Critical Thinking: scenario-based legal analysis, evidence integrity challenges, cross-examination simulations, and ethical dilemma discussions.

MODULE I – Advanced Forensic Frameworks & Expert Witness Standards	**09 Hours**

Topics: Evolution of digital forensics and the legal expertise dimension; forensic investigation lifecycle (identification, preservation, collection, examination, analysis, presentation); international frameworks: NIST SP 800-86, ACPO Good Practice Guide, ISO/IEC 27037; forensic lab accreditation standards (ISO/IEC 17025); chain of custody: documentation, sealing, integrity verification, reproducibility; expert witness qualifications, roles, and responsibilities; Daubert and Frye standards for scientific evidence; forensic readiness planning; order of volatility in evidence acquisition.

Applications: Law enforcement digital investigations, corporate incident response, regulatory compliance audits, expert witness testimony preparation.

AI Integration: AI-assisted case triage and prioritization, automated hash verification workflows, intelligent keyword and entity extraction from forensic datasets.

Authentic Intelligence: Legal boundaries of evidence collection, ethical duties of an expert witness (impartiality, disclosure), risks of cognitive bias and AI-driven false positives in forensic analysis.

MODULE II – Advanced Disk, File System & Artifact Forensics	**09 Hours**

Topics: Advanced file system internals: FAT32, NTFS (MFT, $LogFile, $UsnJrnl), EXT4 (inodes, journal), APFS (snapshots, encryption), exFAT; disk imaging: dd, FTK Imager, Guymager, dcfldd; file carving: Foremost, Scalpel, PhotoRec; metadata forensics: ExifTool, timestamps, MAC(b) times; slack space, unallocated space, and alternate data streams (ADS); deleted file recovery and anti-forensics detection; Windows Registry forensics: hive structure, ShellBags, UserAssist, MRU lists, Amcache; browser and email artifact forensics; prefetch and LNK file analysis.

Applications: Data recovery investigations, insider threat analysis, corporate espionage cases, deleted evidence retrieval, anti-forensics defeat.

AI Integration: Automated file classification of carved artifacts, AI-assisted timeline generation from file system events, anomaly detection in Registry and metadata patterns.

Authentic Intelligence: Legal requirements for write-blocked imaging, admissibility of hash-verified disk images, risks of improper media handling, documentation standards for disk evidence in court.

MODULE III – Advanced Memory, Live & Endpoint Forensics	**09 Hours**

Topics: Memory architecture: RAM, virtual address space, kernel vs. user space, heap and stack analysis; volatile data: running processes, open network connections, loaded DLLs, encryption keys in memory; memory dump acquisition tools: WinPmem, LiME, DumpIt, FTK Imager Live; Volatility 3 framework: pslist, pstree, netscan, malfind, dlllist, cmdline plugins; detecting process injection (DLL injection, process hollowing), rootkits, and fileless malware; endpoint forensics: Windows Event Logs (EVTX), Sysmon, PowerShell logging, scheduled tasks, autoruns; Linux forensics: /proc filesystem, bash history, cron jobs, log files; triage frameworks: KAPE, Velociraptor for rapid endpoint artifact collection.

Applications: Live system triage, APT detection and attribution, ransomware incident response, insider threat investigation, fileless malware hunting.

AI Integration: AI-based anomaly detection in process trees and Event Logs, ML-assisted rootkit and fileless malware identification, automated IOC extraction from memory dumps and endpoint telemetry.

Authentic Intelligence: Legal implications of volatile evidence admissibility, authorization requirements for live memory acquisition, privacy considerations of full memory capture, chain of custody for live triage data.

MODULE IV – Advanced Network, Cloud & Enterprise Forensics	**09 Hours**

Topics: Advanced packet capture and protocol analysis: Wireshark, tcpdump, tshark, Zeek/Bro; protocol forensics: HTTP/S, DNS tunneling, SMB lateral movement, FTP, SMTP, IRC C2; log analysis and correlation: firewall logs, IDS/IPS alerts, web server logs, Windows Event forwarding; session reconstruction, data exfiltration pattern recognition, and C2 traffic identification; NetFlow analysis, SIEM integration (Splunk, ELK); cloud forensics: AWS CloudTrail, Azure Monitor, GCP Audit Logs, S3/Blob forensics, IAM access trails, container and serverless forensics; SaaS forensics: Microsoft 365, Google Workspace audit logs; enterprise forensics: Active Directory artifacts, lateral movement indicators, SIEM-based threat hunting; legal challenges: jurisdiction, lawful interception, encrypted traffic, MLAT requests for cross-border evidence.

Applications: Cyber-attack attribution, data exfiltration investigations, cloud incident response, APT campaign reconstruction, enterprise breach investigation, cross-border evidence requests.

AI Integration: ML-based network traffic anomaly detection, AI-assisted multi-source log correlation, automated PCAP analysis and threat hunting, AI-driven cloud log anomaly scoring.

Authentic Intelligence: Jurisdictional complexity in cloud forensics, lawful interception and MLAT procedures, handling encrypted traffic and VPN evidence, SaaS provider legal cooperation, privacy law implications (GDPR, DPDP Act).

MODULE V – Legal Expertise, Cyber Law & Expert Testimony	**09 Hours**

Topics: Information Technology Act 2000 and amendments (IT Amendment Act 2008); Indian Evidence Act and the Bharatiya Sakshya Adhiniyam 2023 (digital evidence provisions); Digital Personal Data Protection Act 2023 (DPDP Act); expert witness role: qualifications, court etiquette, examination-in-chief, cross-examination, re-examination; search and seizure procedures: IT Act Sec. 69, 69A, 79; CrPC Sec. 91, 93, 165; international frameworks: Budapest Convention, MLAT; forensic report writing: executive summary, methodology, findings, conclusions, annexures; admissibility standards: relevancy, authenticity, reliability, best evidence rule, Section 65B Indian Evidence Act certificate; preparing chain of custody affidavits; ethics of a forensic expert: impartiality, disclosure obligations, professional indemnity; landmark Indian cybercrime case studies.

Applications: Preparing expert witness testimony for civil and criminal proceedings, drafting Section 65B certificates, advising law enforcement on lawful evidence collection, corporate legal compliance consulting, cross-border digital evidence requests.

AI Integration: AI-assisted forensic report drafting, automated citation of relevant legal sections and case law, LLM-based legal research assistance for forensic experts.

Authentic Intelligence: Obligations and liabilities of a forensic expert under Indian law, consequences of evidence tampering and perjury, professional ethics, impartiality, and avoiding conflicts of interest.

Course Outcomes

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

COs	Description	Bloom's Level

CO1	Explain advanced forensic frameworks, expert witness standards, and chain of custody requirements aligned with NIST, ACPO, and ISO/IEC 27037 guidelines.	**L2**
CO2	Apply advanced disk, file system, Registry, and memory forensic techniques using industry-standard tools to acquire, preserve, and analyze digital evidence.	**L3**
CO3	Conduct advanced network, cloud, and enterprise forensic investigations including protocol analysis, multi-source log correlation, and cross-jurisdictional evidence handling.	**L4**
CO4	Perform advanced mobile, IoT, and embedded device forensic acquisitions and conduct malware analysis using static, dynamic, sandbox, and reverse engineering techniques.	**L3**
CO5	Evaluate digital evidence for legal admissibility under Indian and international law, draft forensic investigation reports, Section 65B certificates, and deliver expert witness testimony.	**L5**

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**1**	**2**
CO1	3	2	1	3	1	3	–	3	1	2	2	3	2
CO2	3	3	2	3	3	1	–	1	2	1	2	3	3
CO3	3	3	3	3	3	2	–	2	2	1	3	3	3
CO4	3	3	2	3	3	1	–	1	2	1	3	3	3
CO5	2	2	1	3	1	3	–	3	2	3	2	3	2

TEXT BOOKS:

- Digital Forensics with Open Source Tools – Cory Altheide & Harlan Carvey, Syngress, 2011.
- The Art of Memory Forensics – Andrew Case, Jamie Levy & AAron Walters, Wiley, 2014.

REFERENCE BOOKS:

- Network Forensics: Tracking Hackers through Cyberspace – Sherri Davidoff & Jonathan Ham, Prentice Hall, 2012.

- File System Forensic Analysis – Brian Carrier, Addison-Wesley, 2005; Cybercrime and the Law – Susan W. Brenner, Northeastern University Press, 2012.

RECOMMENDED TOOLS

- Disk & File System: Autopsy, FTK Imager, Guymager, dcfldd, Foremost, Scalpel, ExifTool, RegRipper
- Memory & Endpoint: Volatility 3, WinPmem, LiME, DumpIt, KAPE, Velociraptor
- Network & Cloud: Wireshark, tcpdump, tshark, Zeek, Splunk, ELK Stack, AWS CloudTrail Viewer
- Mobile & IoT: ADB, Cellebrite UFED (demo), iBackupBot, Magnet AXIOM (trial), DB Browser for SQLite
- Malware & RE: Any.run, Cuckoo Sandbox, PEStudio, CFF Explorer, Ghidra, YARA

Blockchain Technology

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VIII

Course Code	**:**		**Credits**	**:**	03

Hours / Week	:	03	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

The widespread popularity of digital cryptocurrencies has led to the foundation of Blockchain, which is fundamentally a public digital ledger to share information in a trustworthy and secure way. This course includes the fundamental design and architectural primitives of Blockchain, consensus protocols, types of the Blockchain system and the security aspects, along with various use cases from different application domains.

Course Objectives:

This course will enable students:

1. Understand fundamentals of blockchain and be able to explain cryptographic concepts underlying blockchain in layman terminology.
2. Design and evaluate the concept of smart contracts and how they can be used to construct Decentralized Applications (DApps).
3. Applying blockchain in different application domains that are transforming society.
4. Demonstrate how to perform compiling, migrating, testing, and deploying the blockchain applications on the decentralised network.
5. Adapt the advanced concepts of blockchain programming language and tools to develop complex blockchain applications.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with traditional lecture method, different types of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I	**09 Hours**

Introduction to Blockchain Technology, Bitcoin Blockchain, Blockchain Architecture, Conceptualization, Blockchain components, Cryptocurrencies, Characteristics of cryptocurrencies, Alt coins, Crypto wallets, Creation of Blocks, Wallet Transactions, Transaction details in a Block, Merkle Tree, Hash functions, pseudo random numbers, Puzzle friendly and collision resistant hash, public key cryptosystem, Generation of keys, Digital signatures, Zero-knowledge systems.

Applications: Cryptocurrency transactions, Secure digital payments

AI Integration: Fraud detection models, Blockchain analytics tools

Authentic Intelligence: Trust evaluation in financial transactions, Human validation of digital signatures	
MODULE – II	**09 Hours**
Blockchain types-Public Blockchain, Private Blockchain, Federated Blockchain, Permissionless, Permissioned Blockchain Networks, Ethereum blockchain, Go Ethereum, Gas, Gas price, Gas Limit, ETH, MetaMask, Public Test Networks, set up a Ethereum node using Geth, Mining in Blockchain, Steps in Mining, Double spending, PoW, Hashcash, Attacks on Bitcoin, Sybil Attacks, 51% Attack, eclipse attacks, DDoS Attacks, Replay Attacks, Byzantine fault, node failure. **Applications:** Decentralized applications (DApps), Secure blockchain networks **AI Integration**: Network anomaly detection, Intrusion detection systems **Authentic Intelligence:** Governance in decentralized networks, Human monitoring of attacks	
MODULE – III	**09 Hours**
Proof of Stake, Difference between PoW vs PoS, Byzantine General Problem, BFT (Byzantine fault tolerance), PBFT (Practical Byzantine fault tolerance), Delegated Proof of Stack, Paxos Consensus algorithm, Raft Algorithm, Solo Miner, Pool Miners, Smart contracts in Blockchain, Solidity, Data types in solidity, Operators, State variables, Global Variables, Local variables. **Applications:** Consensus-driven systems, Automated digital agreement **AI Integration:** AI-based consensus optimization, Smart contract vulnerability detection **Authentic Intelligence**: Ethical decision-making in automated contracts, Trust in consensus participation	
MODULE – IV	**09 Hours**
Remix, Compilation of smart contracts, Deployment environments, JavaScript Environment, Injected Web3, Web3 Provider, Solidity arrays, Solidity functions, Structs in solidity, Inheritance, Special variables, Solidity mapping, Function overloading, Personal Blockchain network, Ganache, Contract deployment to Ganache network, Modifiers in solidity, Events. **Applications:** DeFi platforms, Blockchain-based applications **AI Integration:** Smart contract auditing tools, AI-based bug detection **Authentic Intelligence**: Human validation of contract logic, Ethical auditing of smart contracts	
MODULE – V	**09 Hours**

Hyperledger: Projects under Hyperledger, Hyperledger reference architecture, Hyperledger design principles, Hyperledger Fabric, Hyperledger Sawtooth, Case study: Blockchain in IoT, healthcare, and finance.

Applications: Enterprise blockchain systems, Supply chain and healthcare

AI Integration: Predictive analytics with blockchain, AI-enabled supply chain tracking

Authentic Intelligence: Decision-making in enterprise blockchain, Ethical data sharing

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Explain blockchain fundamentals, cryptographic mechanisms, and transaction processes.	L2
2	Analyze blockchain architecture, Ethereum ecosystem, and security threats.	L3, L4
3	Apply consensus mechanisms and develop basic smart contracts.	L3, L4, L5
4	Evaluate and deploy smart contracts using blockchain tools.	L3, L4, L5
5	Design blockchain solutions for real-world applications.	L3, L4, L5, L6

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	**3**	**2**	**1**	-	-	-	2	-	-	-	**1**	**2**	**1**

CO2	**3**	**3**	**2**	**2**	**2**	**-**	**2**	**-**	**-**	**-**	**1**	**3**	**2**
CO3	**3**	**3**	**3**	**2**	**3**	**-**	**2**	**-**	**-**	**-**	**1**	**3**	**3**
CO4	**3**	**3**	**3**	**3**	**3**	**-**	**3**	**-**	**-**	**-**	**1**	**3**	**3**
CO5	**2**	**3**	**3**	**3**	**3**	**-**	**3**	**-**	**-**	**-**	**2**	**3**	**3**

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Bashir, Imran. Mastering blockchain: "Distributed ledger technology, decentralization, and smart contracts explained". Packt Publishing Ltd, 2018.
2. Bettina Warburg, Bill Wanger and Tom Serres, Basics of Blockchain (1 ed.), Independently published, 2019. ISBN 978-1089919445.

REFERENCE BOOKS:

1. Holbrook, Joseph. Architecting enterprise blockchain solutions. John Wiley & Sons, 2020

MOOC courses:

- Bitcoin and Cryptocurrency Technologies (Coursera offered by Princeton University).

  URL: https://www.coursera.org/learn/cryptocurrency#

- Smart Contracts. URL: https://www.coursera.org/learn/smarter-contracts

- Blockchain Platforms: URL: https://www.coursera.org/learn/blockchain-platforms

END POINT SECURITY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER -VIII

Course Code	**:**		**Credits**	**:**	03
Hours / Week	**:**	03	**Total Hours**	**:**	45
L–T–P–J	**:**	3–0–0–0	**CIE+SEE**	**:**	60+40 Marks

Course Vision:

To develop skilled professionals who can protect endpoint devices using modern security practices, ensuring confidentiality, integrity, and availability while proactively defending against evolving cyber threats.

Course Objectives:

This course will enable students:

1. Explain basic networking concepts and security principles .
2. Identify different endpoint types and security requirements .
3. Identify built-in security mechanisms in Windows systems .
4. Utilize Linux security tools to monitor, detect, and mitigate security threats.
5. Design secure network environments using segmentation and access control techniques.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with traditional lecture method, different types of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and role-playing.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I	**09 Hours**

Securing Networks

Topics:

Network Security Fundamentals,Firewalls,IDS/IPS,Access Control Lists (ACLs),VPN Concepts,Secure Network Design,Network Segmentation.

Applications:

- Enterprise Network Protection
- Cloud Security
- Banking and Financial Security
- Healthcare Security Systems
- Government and Defense Networks
- Industrial Control Systems (ICS)

AI Integration:

- AI-based Threat Detection
- Machine Learning for Intrusion Detection
- Behavioral Analytics
- Automated Incident Response
- Predictive Threat Intelligence

Authentic Intelligence:

- Human-driven Cybersecurity Decision Making
- Ethical Security Practices
- Threat Verification and Validation
- Human + AI Collaboration
- Security Awareness and Training

MODULE – II	**09 Hours**

Endpoint Security Framework

Topics:

Endpoint Protection Platforms (EPP), Endpoint Detection & Response (EDR) solutions, antimalware, retrospective security, Indication of Compromise (IOC), antivirus, dynamic file analysis, and endpoint-sourced telemetry.

Applications:

- Enterprise Endpoint Protection
- Banking and Financial Security
- Healthcare Data Protection

AI Integration:

- AI-driven Threat Detection
- Machine Learning-based Malware Analysis
- Predictive Security Analytics
- Automated Threat Hunting

Authentic Intelligence:

- Human-led Threat Investigation
- Expert Validation of AI Alerts
- Ethical Cybersecurity Practices
- Analyst-driven Incident Response

MODULE – III	**09 Hours**

Windows Operating System Security

Topics:

Windows Security Features,User Account Control,NTFS Permissions,Windows Defender,Group Policies,Patch Management.

Applications:

- Enterprise Windows Security Management
- Secure User Access Control
- Data Protection in Organizations
- Endpoint Hardening
- Centralized Security Administration

AI Integration:

- .AI-based Threat Detection in Windows Systems
- Intelligent Malware Analysis
- Automated Patch Management
- Predictive Vulnerability Assessment

Authentic Intelligence:

- Human-supervised Security Operations
- Expert Analysis of Security Incidents
- Ethical System Administration

MODULE – IV	**09 Hours**

Linux Overview and Security

Topics:

Linux Basics,File Permissions,Linux User Management,Linux Security Tools,SSH Security,Linux Hardening

Applications:

- Secure Linux Server Administration
- Cloud Infrastructure Protection
- Web Server Security
- Database Security
- Enterprise Linux Endpoint Protection

AI Integration:

- AI-driven Threat Detection in Linux Systems

- Intelligent Log Analysis
- Automated Vulnerability Scanning
- Machine Learning-based Intrusion Detection

Authentic Intelligence:

- Human-led Security Monitoring
- Expert-based Linux Incident Analysis
- Ethical Linux Administration
- Manual Validation of Security Events

MODULE – V	**09 Hours**

IoT Endpoint Protection Techniques

Topics:

Network Segmentation,Zero Trust Security,Endpoint Detection and Response (EDR),Intrusion Detection Systems (IDS),Secure Firmware Updates,Device Hardening,Vulnerability Assessment,Continuous Monitoring,IoT Security Protocols.

Applications:

- Smart Home Security Systems
- Industrial IoT (IIoT) Protection
- Smart City Infrastructure Security
- Healthcare IoT Monitoring Systems

AI Integration:

- AI-based anomaly detection in IoT networks
- Machine learning for threat prediction
- Behavioral analytics for devices
- Automated intrusion detection and response

Authentic Intelligence:

- Human-led threat validation and investigation
- Expert-driven security decision making
- Ethical oversight of AI security systems
- Manual confirmation of critical alerts

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Understand secure network design principles .	L2
2	understand endpoint security solutions using EPP and EDR technologies, detect malware and indicators of compromise .	L2
3	Understand the architecture and core security mechanisms of the Microsoft Windows operating system.	L2
4	Understand Linux file systems and implement file and directory permission mechanisms for secure access control.	L2
5	Understand the fundamentals of secure network architecture and modern cybersecurity principles for connected systems and IoT environments.	L2

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	2	1	2	2	3	1			2	2		2	2
CO2	2	1	2	2	3	1			2	2		2	2
CO3	2	1	2	2	3	1			2	2		2	2
CO4	2	1	2	2	3	1			2	2		2	2

CO5	2	1	2	2	3	1			2	2		2	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Mark Kadrich, "Endpoint Security", Addison-Wesley — 1st ed .ISBN 0-321-43695-4
2. Axel Buecker, Alisson Campos, Peter Cutler, Andy Hu, Garreth Jeremiah, Toshiki Matsui, Michal Zarakowski, Endpoint Security and Compliance Management, IBM Red Books, 2012.

REFERENCE BOOKS:

1. Andrew Avanessian, The Endpoint Security Paradox, 2016.

E-Resources:

1. https://www.ibm.com/topics/endpoint-security
2. https://www.coursera.org/articles/endpoint-security
3. https://skillsforall.com/course/endpoint-security?courseLang=en-US
4. https://www.sans.org/cyber-security-courses/security-essentials-network-endpoint-cloud/

Mini Projects

Students will design practical auditing/compliance-based systems such as:

- **Antivirus Scanner Simulation**
- **Password Strength Checker**
- **USB Device Monitoring System**
- Basic Firewall Rule Simulator
- Keylogger Detection Tool

Students should demonstrate the following:

- Risk analysis
- Tool usage
- Compliance mapping
- Report generation

Recommended Tools

- Microsoft Defender Antivirus
- Symantec Endpoint Protection
- McAfee Endpoint Security

Activity Based Learning (Suggested Activities in Class)

1. **Interactive Quizzes and Games:** Create interactive quizzes or games related to endpoint security concepts, terminology, and best practices. This can make learning more engaging and help reinforce key concepts in a fun and interactive way.
2. **Role-Playing Scenarios:** Divide students into groups and assign them different roles such as IT administrators, employees, and attackers. Create scenarios where they have to respond to security incidents like phishing emails or malware infections.
3. **Case Study Analysis:** Provide case studies of real-world endpoint security breaches or successful defense strategies. Have students analyze the cases in groups, identify key issues, and propose solutions or preventive measures.
4. **Group Projects:** Assign group projects where students have to design and present comprehensive endpoint security plans for fictional organizations or scenarios. This encourages collaboration, critical thinking, and practical application of concepts learned in class.

Industrial Digital Twin

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER –VIII

Course Code	:		**Credits**		3
Hours / Week	:		**Total Hours**		45
L–T–P–J	:	3–0–0–0	**CIE+SEE**		60+40 Marks

Course Vision:

To develop the ability to understand, design, and analyze secure communication systems using principles of quantum mechanics and cryptography for next-generation cyber security applications.

Course Objectives:

This course will enable students:

1. To summarize the fundamentals of Digital Twin and Industrial IoT systems.
2. To understand data acquisition, modeling, and simulation of physical systems.
3. To apply analytics and AI techniques for real-time monitoring and optimization.
4. To analyze system performance using Digital Twin frameworks.
5. To evaluate industrial applications, challenges, and security aspects.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. Lecture method along with traditional lecture delivery may be adopted to explain Digital Twin concepts effectively.
2. Interactive Teaching: incorporating brainstorming, discussions, group work, and system design activities.
3. Showing video/animation films to demonstrate industrial processes and Digital Twin models.
4. Encourage Collaborative (Group Learning) through case studies and industrial problem-solving tasks.
5. Demonstrations using simulation tools and IoT platforms.
6. To develop critical thinking through quizzes and real-world industrial scenario analysis.

MODULE – I	**09 Hours**

Foundations of Digital Twin and Industrial Systems

Topics: Introduction to Digital Twin, Evolution and Applications of Digital Twins, Types of Digital Twins, Components and Architecture of Digital Twin Systems, Industrial IoT (IIoT), Cyber-Physical Systems (CPS), Data Acquisition and Sensors, Communication Protocols in IIoT, Edge Computing and Cloud Integration, Real-Time Data Processing, Simulation and Modeling Techniques, Artificial Intelligence and Machine Learning in Digital Twins.

Applications: Smart manufacturing, predictive maintenance, real-time monitoring of industrial systems.

AI Integration: Introduction to data-driven modeling, basic analytics using Python, integration of sensor data with AI models.

Authentic Intelligence: Challenges in real-time data acquisition, system integration issues, limitations in modeling physical systems accurately.

NVIDIA DLI Courses (Relevant to this Module):

1. Accelerating End-to-End Data Science Workflows (8 hrs) | Path: Data Science Training - Accelerated Data Science Foundations

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-01+V2

2. Best Practices in Feature Engineering for Tabular Data With GPU Acceleration (2 hrs) | Path: Accelerated Data Science Foundations

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-06+V1

MODULE – II	**09 Hours**

Data Modeling and Simulation

Topics: System Modeling Techniques, Mathematical and Simulation Models, Simulation Methods and Tools, Data Preprocessing Techniques, Time-Series Data Analysis, Virtual Representation of Physical Systems, Dynamic System Modeling, Digital Thread and Data Flow, Signal Processing for Sensor Data, Real-Time Monitoring and Control, State Estimation Techniques, Model Validation and Verification, Event-Driven Simulation, Data Synchronization Techniques.

Applications: Process optimization, system behavior prediction, simulation of industrial workflows.

AI Integration: Machine learning models for predictive analysis, simulation using Python tools, anomaly detection.

Authentic Intelligence: Data quality issues, risks of incorrect modeling, challenges in synchronization between physical and virtual systems.

MODULE – III	**09 Hours**

Digital Twin Implementation and Platforms

Topics: Digital Twin Frameworks, Cloud and Edge Computing, IoT Platforms and Ecosystems, Data Integration Techniques, APIs and Middleware, Communication Protocols (MQTT, CoAP, OPC-UA), Distributed Computing Architectures, Real-Time Data Streaming, Data Storage and Management, Interoperability Standards, Service-Oriented Architecture (SOA), Microservices for Digital Twins**.**

Applications: Smart factories, supply chain optimization, industrial automation.

AI Integration: Use of AI for real-time decision-making, integration with cloud-based analytics platforms.

Authentic Intelligence: Latency issues, scalability challenges, data security concerns in cloud environments.

NVIDIA DLI Free Courses (Relevant to this Module):

1. **Accelerating Clustering Algorithms to Achieve the Highest Performance** (2 hrs) | Path: Data Science Training – Accelerated Data Science Foundations

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-04+V1

MODULE – IV	**09 Hours**

Analytics, Optimization and Control

Topics: Predictive Maintenance, Optimization Techniques, Intelligent Control Systems, Data Visualization Techniques, Real-Time Monitoring and Analytics, Condition Monitoring Systems, Fault Detection and Diagnostics, Machine Learning for Predictive Analysis, Reliability and Performance Optimization, Process Automation, Decision Support Systems, Supervisory Control and Data Acquisition (SCADA), Human–Machine Interface (HMI).

Applications: Fault detection, performance optimization, intelligent control systems.

AI Integration: Deep learning models, reinforcement learning for optimization, visualization tools for insights.

Authentic Intelligence: Overfitting risks, model reliability issues, decision-making challenges in dynamic environments.

NVIDIA DLI Courses (Relevant to this Module):

1. **Exploring Adversarial Machine Learning** (8 hrs) | Path: Deep Learning Training – AI Security Engineering & Federated ML

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-03+V1

MODULE – V	**09 Hours**

Security, Challenges and Industrial Applications

Topics: Security in Digital Twin Systems, Cyber Threats in IIoT, Data Privacy and Protection, Ethical Issues in Digital Twin Technology, Risk Assessment and Threat Modeling, Secure Communication Protocols, Authentication and Access Control Mechanisms, Encryption Techniques for IoT and Digital Twins, Network Security in Industrial Systems**.**

Applications: Secure industrial operations, risk management, digital transformation strategies.

AI Integration: AI-based anomaly detection, predictive security analysis, automated monitoring systems.

Authentic Intelligence: Security vulnerabilities, ethical concerns, challenges in large-scale deployment.

NVIDIA DLI Free Courses (Relevant to this Module):

1. **Accelerate Data Science Workflows with Zero Code Changes** (1 hr) | Path: Data Science Training – Data Preparation for Model Training

https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+T-DS-03+V1

Course Outcome

Course Outcomes		**Bloom's Taxonomy**

(COs)	Description	Level
At the end of the course the student will be able to:		
1	Recall basic concepts of Digital Twin and industrial systems.	L1
2	Describe Digital Twin architecture and data modeling techniques.	L2
3	Apply simulation and AI techniques for industrial system analysis.	L3
4	Analyze system performance and optimization using Digital Twin models.	L4
5	Evaluate security, challenges, and real-world industrial applications.	L5

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	1	1	-	-	-	-	-	-	-	-	1	1	1
CO2	2	2	1	-	-	-	-	-	-	-	1	2	2
CO3	3	2	1	1	1	2	1	-	2	1	1	2	2
CO4	3	2	1	1	1	2	1	-	2	1	1	2	2
CO5	3	2	1	1	1	2	1	-	2	1	1	2	2

3: Substantial (High) 2: Moderate (Medium) 1: Poor (Low)

TEXT BOOKS:

1. Digital Twin Driven Smart Manufacturing – Fei Tao & Qinglin Qi, Academic Press, 1st Edition.
2. Industrial Internet of Things – Sabina Jeschke, Springer, 1st Edition.

REFERENCE BOOKS:

1. Designing the Digital Transformation – Gary O'Donnell, Springer.
2. Smart Manufacturing Systems – Masoud Soroush, Elsevier..

RECOMMENDED TOOLS

Programming: Python (NumPy, Pandas, TensorFlow) – Google Colab/ Jupyter Notebook

IoT Platforms: ThingWorx, AWS IoT, Azure IoT Hub

Simulation Tools: MATLAB/Simulink, AnyLogic

Visualization: Power BI, Tableau, Grafana

Cloud Platforms: AWS, Azure

AI Assistants: GitHub Copilot, ChatGPT, Claude