



SIDDAGANGA INSTITUTE OF TECHNOLOGY, TUMAKURU

(An autonomous institution affiliated to VTU, Belagavi, Approved by AICTE, New Delhi, Accredited by NAAC with 'A++' grade & ISO 9001:2015 Certified)

B.E. in Computer Science and Engineering (AI & ML)

SCHEME OF TEACHING AND EXAMINATION (2022 Scheme)

VII Semester

Sl. No.	Course and Course Code		Course Title	Teaching / Paper setting Dept.	Teaching hrs./week				Examination			Credits	
					Lecture	Tutorial	Practical/ Drawing	Self-Study Component	Duration in hrs.	CIE Marks	SEE Marks		Total Marks
					L	T	P	S					
1.	IPCC	S7CCSI01	Artificial Neural Network and Deep Learning (I)		42	0	28		3	50	50	100	4
2.	IPCC	S7CII01	Generative AI and Prompt Engineering(I)		42	0	28		3	50	50	100	4
3.	PCC	S7CI01	Federated Learning		42	28	0		3	50	50	100	4
4.	PEC		Professional Elective Course-III		42	0	0		3	50	50	100	3
5.	OEC		Open Elective Course-II		42	0	0		3	50	50	100	3
6.	PROJ	S7CIMP	Major Project Phase II		0	0	12		3	100	100	200	6
			Total							350	350	700	24
		AAP	AICTE Activity Points (Applicable for both Regular and Lateral Entry students)		40 hours community service to be documented and produced for the examination								

Note: **IPCC:** Integrated Professional Core Course, **PCC:** Professional Core Course; **PEC:** Professional Elective Course; **OEC:** Open Elective Course; **PROJ:** Project Phase –II; **L:** Lecture, **T:** Tutorial, **P:** Practical **S= SDA:** Skill Development Activity, **CIE:** Continuous Internal Evaluation, **SEE:** Semester End Evaluation.

Professional Elective Course (PEC) (Offered by the Department)

S7CCSPE01	Explainable and Responsible AI	S7CCSPE04	AI in Data Security & Privacy
S7CCSPE02	Robotic Process Automation	S7CCSPE05	Blockchain traced AI
S7CCSPE03	Agentic AI- Foundations and Applications		

Note: VII and VIII semesters of IV years of the program

- 1) Institutions can swap the VII and VIII Semester Schemes of Teaching and Examinations to accommodate research internships/ industry internships after the VI semester.
- 2) Credits earned for the courses of VII and VIII Semester Scheme of Teaching and Examinations shall be counted against the corresponding semesters whether the VII or VIII semesters is completed during the beginning of the IV year or the later part of IV years of the program.

Professional Core Course (IPCC): Refers to Professional Core Course Theory Integrated with practical of the same course. Credit for IPCC can be 04 and its Teaching–Learning hours (L : T : P) can be considered as (3 : 0 : 2) or (2 : 2 : 2). The theory part of the IPCC shall be evaluated both by CIE and SEE. The practical part shall be evaluated by only CIE (no SEE). However, questions from the practical part of IPCC shall be included in the SEE question paper. For more details, the regulation governing the Degree of Bachelor of Engineering (B.E.) 2022-23 may please be referred.

Professional Elective Courses (PEC): A professional elective (PEC) course is intended to enhance the depth and breadth of educational experience in the Engineering and Technology curriculum. Multidisciplinary courses that are added supplement the latest trend and advanced technology in the selected stream of Engineering. Each group will provide an option to select one course. The minimum number of students' strengths for offering a professional elective is 10. However, this conditional shall not be applicable to cases where the admission to the program is less than 10.

Open Elective Courses: Students belonging to a particular stream of Engineering and Technology are not entitled to the open electives offered by their parent Department. However, they can opt for an elective offered by other Departments, provided they satisfy the prerequisite condition if any. Registration to open electives shall be documented under the guidance of the Program Coordinator/ Advisor/Mentor. The minimum numbers of students' strength for offering Open Elective Course is 10. However, this condition shall not be applicable to class where the admission to the program is less than 10.

Project Work: The objective of the Project work is

- i) To encourage independent learning and the innovative attitude of the students.
- ii) To develop interactive attitude, communication skills, organization, time management, and presentation skills.
- iii) To impart flexibility and adaptability.
- iv) To inspire team working.
- v) To expand intellectual capacity, credibility, judgment and intuition.
- vi) To adhere to punctuality, setting and meeting deadlines.
- vii) To install responsibilities to oneself and others.
- viii) To train students to present the topic of project work in a seminar without any fear, face the audience confidently, enhance communication skills, involve in group discussion to present and exchange ideas.

CIE procedure for Project Work:

- 1) Single discipline: The CIE marks shall be awarded by a committee consisting of the Head of the concerned Department and two senior faculty members of the Department, one of whom shall be the Guide.
The CIE marks awarded for the project work, shall be based on the evaluation of the project work Report, project presentation skill, and question and answer session in the ratio 50:25:25. The marks awarded for the project report shall be the same for all the batch mates.
- 2) Interdisciplinary: Continuous Internal Evaluation shall be group-wise at the college level with the participation of all guides of the college. Participation of external guide/s, if any, is desirable. The CIE marks awarded for the project work, shall be based on the evaluation of project work Report, project presentation skill, and question and answer session in the ratio 50:25:25. The marks awarded for the project report shall be the same for all the batch mates.

SEE procedure for Project Work: SEE for project work will be conducted by the two examiners appointed by the University. The SEE marks awarded for the project work shall be based on the evaluation of project work Report, project presentation skill, and question and answer session in the ratio 50:25:25.



SIDDAGANGA INSTITUTE OF TECHNOLOGY, TUMAKURU

(An autonomous institution affiliated to VTU, Belagavi, Approved by AICTE, New Delhi, Accredited by NAAC with 'A++' grade & ISO 9001:2015 Certified)

B.E. in Computer Science and Engineering (AI & ML)

SCHEME OF TEACHING AND EXAMINATION (2022 Scheme)

VIII Semester

Sl. No.	Course and Course Code		Course Title	Teaching / Paper setting Dept.	Teaching hrs./week				Examination			Credits		
					Lecture	Tutorial	Practical/ Drawing	Self-Study Component	Duration in hrs.	CIE Marks	SEE Marks		Total Marks	
					L	T	P	S						
1.	PEC		Professional Elective (Online Courses)		3	0	0		3	50	50	100	3	
2.	OEC		Open Elective (Online Courses)		0	2	0		3	50	50	100	3	
3.	INT		Internship (Industry/Research) (14-20 weeks)		0	0	12		3	100	100	200	10	
			Total							200	200	400	16	
		AAP	AICTE Activity Points (Applicable for both Regular and Lateral Entry students)	40 hours community service to be documented and produced for the examination										
Note: PEC: Professional Elective Course; OEC: Open Elective Course (Online); INT: Industry Internship / Research Internship / Rural Internship L: Lecture, T: Tutorial, P: Practical S= SDA: Skill Development Activity, CIE: Continuous Internal Evaluation, SEE: Semester End Evaluation.														
Professional Elective (Online Courses – suggested by BoS, NPTEL)														
			Human Computer Interactions											
			GPU Architectures and Programming											
			Affective Computing											
			Introduction to Industry 4.0 and Industrial Internet of Things											
			Ethical Hacking											
Open Elective (Online Courses – suggested by BoS, NPTEL)														
			AI in Human Resource Management											
			AI in Product Management											
			Food Science and Technology											
			Carbon Accounting and Sustainable Designs in Product Lifecycle Management											
			Six sigma											
Note: VII and VIII semesters of IV years of the program														

- 1) Institutions can swap the VII and VIII Semester Schemes of Teaching and Examinations to accommodate research internships/ industry internships after the VI semester.
- 2) Credits earned for the courses of VII and VIII Semester Scheme of Teaching and Examinations shall be counted against the corresponding semesters whether the VII or VIII semester is completed during the beginning of the IV year or the later part of IV years of the program.

Elucidation:

At the beginning of IV years of the program i.e., after VI semester, VII semester classwork and VIII semester Research Internship /Industrial Internship / Rural Internship shall be permitted to be operated simultaneously by the University so that students have ample opportunity for an internship. In other words, a good percentage of the class shall attend VII semester classwork and a similar percentage of others shall attend to Research Internship or Industrial Internship or Rural Internship.

Research/Industrial /Rural Internship shall be carried out at an Industry, NGO, MSME, Innovation center, Incubation center, Start-up, center of Excellence (CoE), Study Centre established in the parent institute and /or at reputed research organizations/institutes.

The mandatory Research internship /Industry internship / Rural Internship is for 14 to 20 Weeks. The internship shall be considered as a head of passing and shall be considered for the award of a Degree. Those, who do not take up/complete the internship shall be declared to fail and shall have to complete it during the subsequent University examination after satisfying the internship requirements.

Research internship: A research internship is intended to offer the flavor of current research going on in the research field. It helps students get familiarized with the field and imparts the skill required for carrying out research.

Industry internship: Is an extended period of work experience undertaken by students to supplement their Degree for professional development. It also helps them learn to overcome unexpected obstacles and successfully navigate organizations, perspectives, and cultures. Dealing with contingencies helps students recognize, appreciate, and adapt to organizational realities by tempering their knowledge with practical constraints.

Rural Internship: Rural development internship is an initiative of Unnat Bharat Abhiyan Cell, RGIT in association with AICTE to involve students of all departments studying in different academic years for exploring various opportunities in techno-social fields, to connect and work with Rural India for their upliftment.

The faculty coordinator or mentor has to monitor the student's internship progress and interact with them to guide for the successful completion of the internship.

The students are permitted to carry out the internship anywhere in India or abroad. University shall not bear any expenses incurred in respect of the internship.

With the consent of the internal guide and Principal of the Institution, students shall be allowed to carry out the internship at their hometown (within or outside the state or abroad), provided favorable facilities are available for the internship and the student remains regularly in contact with the internal guide. University shall not bear any cost involved in carrying out the internship by students. However, students can receive any financial assistance extended by the organization.

Professional Elective /Open Elective Course: These are ONLINE courses suggested by the respective Board of Studies. Details of these courses shall be made available for students on the VTU web portal.

B.E. COMPUTER SCIENCE & ENGINEERING
(ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING)
 Outcome Based Education (OBE) and Choice Based Credit System (CBCS)
SEMESTER - VII

ARTIFICIAL NEURAL NETWORK AND DEEP LEARNING (I)

Course Code	S7CCSI01	CIE Marks	50
Teaching Hours/Week (L:T:P)	(3:0:0)	SEE Marks	50
Credits	4	Exam Hours	3
Lecture Hours	42Hrs	Practical Hours	28hrs

Course objectives: This course will enable students to:

1.	Get introduced the fundamental concepts of neural networks, including neuron models, network architectures, and biological inspiration
2.	Analyze and implement single-layer and multilayer perceptron models, with a focus on learning algorithms like back propagation.
3.	Explore techniques for improving neural network training through regularization, data augmentation, and optimization strategies.
4.	Understand the structure and functioning of Convolutional Neural Networks (CNNs) and their role in processing spatial data.
5.	Examine sequence modeling using Recurrent Neural Networks (RNNs), including LSTM and encoder-decoder architectures for temporal data.

UNIT I

8 Hours

Introduction: What is a Neural Network?, The Human Brain, Models of a Neuron, Neural Networks Viewed As Directed Graphs, Feedback, Network Architectures, Rosenblatt's Perceptron: Introduction, Perceptron, The Perceptron Convergence Theorem, Relation Between the Perceptron and Bayes Classifier for a Gaussian Environment.

UNIT II

8 Hours

Multilayer Perceptrons: Introduction, Batch Learning and On-Line Learning, The Back-Propagation Algorithm, XOR Problem, Heuristics for Making the Back- Propagation Algorithm Perform Better, Back Propagation and Differentiation.

UNIT III

8 Hours

Regularization for Deep Learning: Parameter Norm Penalties - L2 Parameter Regularization, Dataset Augmentation, Semi-Supervised Learning. Optimization for Training Deep Models: Challenges in Neural Network Optimization – Ill Conditioning, Local Minima, Plateaus, Saddle Points and Other Flat Regions.

UNIT IV

8 Hours

Convolution neural networks: The Convolution Operation, Motivation, Pooling, Convolution and Pooling as an Infinitely Strong Prior, Variants of the Basic Convolution Function, Structured Outputs, Data Types, Efficient Convolution Algorithms, Convolutional Networks and the History of Deep Learning.

UNIT V

8 Hours

Sequence Modeling: Recurrent and Recursive Nets: Unfolding Computational Graphs, Recurrent Neural Networks, Bidirectional RNNs, Encoder-Decoder Sequence-to-Sequence Architectures, Deep Recurrent Networks, Recursive Neural Networks, The Long Short-Term Memory and Other Gated RN

Sl No	Experiments
1	Develop a program for Back propagation learning and applications.
2	Develop a program for single layer and multi-layer perception learning and applications.
3	Develop a program to implement Support Vector Machine algorithm and applications.
4	Develop a program to implement Self Organizing Maps algorithm and applications.
5	Develop a program for construction of Recurrent Neural Network and applications.
6	Develop a program for construction of Deep Neural Network and applications.
7	Develop a program for construction of Convolution Neural Network and applications.
8	Design and implement recurrent neural network and Bayesian network.

Course Outcomes: On Successful completion of this course, students will be able to	
1.	Describe the structure and function of artificial neural networks and relate them to biological neural systems.
2.	Implement perceptron and multilayer perceptron models using learning algorithms such as back propagation.
3.	Apply regularization and optimization techniques to enhance the performance and generalization of deep learning models.
4.	Design and evaluate Convolutional Neural Networks (CNNs) for applications involving image and spatial data processing.
5.	Develop sequence-based models using Recurrent Neural Networks (RNNs), including LSTM and sequence-to-sequence architectures for tasks like language modeling and time series prediction.

Sl. No	Title of the Book	Name of the Authors	Name of the publisher	Edition & Year
Textbooks				
1	Neural networks and Learning Machines	Simon Haykin	Pearson	Third Edition,2016
2	Deep Learning,	Ian Goodfellow, Yoshua Bengio and Aaron Courville	MIT Press	2016
Reference Books				
1	Deep Learning with Python	Francois Chollet	Manning Publications	2021

Course Articulation Matrix (CO-PO and CO_PSO MAPPING)

Course Outcomes	Program Outcomes											PSOs			
	1	2	3	4	5	6	7	8	9	10	11	1	2	3	
CO1	2	2											2		
CO2	2	2	2		2								2		
CO3				2	2								2		
CO4		2											2		
CO5					2								2		
Overall CO	2	2	2	2	2								2		

Program Articulation Matrix:

Course Outcomes	Program Outcomes											PSOs		
	1	2	3	4	5	6	7	8	9	10	11	1	2	3
	2	2	2	2	2							1	2	3

B.E. COMPUTER SCIENCE & ENGINEERING
(ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING)
 Outcome Based Education (OBE) and Choice Based Credit System (CBCS)
SEMESTER - VII

GENERATIVE AI AND PROMPT ENGINEERING(I)

Course Code	S7CII01	CIE Marks	50
Teaching Hours/Week (L:T:P)	(3:0:2)	SEE Marks	50
Credits	3	Exam Hours	3
Lecture Hours	42Hrs	Practical Hours	28Hrs

Course objectives: This course will enable students to:

1	To provide a comprehensive understanding of generative AI models and their applications
2	To explore the key components and workings of LangChain and its comparison with other frameworks
3	To develop skills for building and implementing chatbots using advanced retrieval and vector techniques
4	To introduce the fundamentals and importance of prompt engineering in AI communication
5	To equip students with best practices and strategies for writing effective prompts and addressing common challenges in prompt engineering.

UNIT I

8 Hours

Introducing generative AI: Generative models, Understanding LLMs, What is a GPT?, Other LLMs, Major players, Working of GPT models, Pre-training, Tokenization, Scaling, Conditioning, text-to-image models, LangChain for LLM Apps: Going beyond stochastic parrots, limitations of LLMs, mitigating LLM limitations, LLM app, LangChain

UNIT II

9 Hours

Exploring key components of LangChain, chains, agents, memory, tools, working of LangChain, Comparing LangChain with other frameworks, Summarizing information, Basic prompting Prompt templates, Building a **Chatbot like ChatGPT:** What is a chatbot?, Understanding retrieval and vectors, Embeddings, Vector storage, Vector indexing, Vector libraries, Vector databases, Loading and retrieving in LangChain, Document loaders, Retrievers in LangChain, kNN retriever, PubMed retriever, Custom retrievers.

UNIT III

9 Hours

Implementing a chatbot, Document loader, Vector storage, Memory, LLMs for Data Science, The impact of generative models on data science, Automated data science, Data collection, Visualization and EDA, Preprocessing and feature extraction, The Future of Generative Models, The current state of generative AI, Challenges, Trends in model development, Artificial General Intelligence, Economic consequences, Creative industries and advertising, Education, Law, Manufacturing, Medicine, Military, Societal implications.

UNIT IV

8 Hours

Introduction to ChatGPT, Overview of Large Language Models, Output Formats Generated By ChatGPT, Use Cases for ChatGPT, Differences Between ChatGPT and Web Search, Introduction to Prompt Engineering: Definition of Prompt Engineering, Importance of Prompt Engineering in AI Communications, Overview of the Different Types of Prompts, Understanding the Foundation of Prompt Engineering, Power Up Your Prompts With Effective Verbs, Elevate Your Prompts with Nuances of Tone, Progressive Experimentation for Refining Prompts, Do You Need Programming Skills to Become a Prompt Engineer?

UNIT V	8 Hours
Writing Effective Prompts, Key Attributes of Good Prompt Writing, Tips for Getting the Most Out of Prompt Responses, Best Practices in Prompt Engineering: Understanding the Nuances of Language & Tone, Testing & Iterating Prompts for Improved Performance, Incorporating Feedback from AI Models to Refine Prompts, Enhancing Reliability of Responses, Give More "Think Time" to the Model, Staying Up to Date with the Latest Advancements, Tips for Getting the Most Out of Prompt Responses, Challenges in Prompt Engineering: Addressing Common Challenges & Pitfalls, Strategies for Improving Prompt Effectiveness, Ethical Considerations in Prompt Engineering.	

Course Outcomes: On Successful completion of this course, students will be able to	
1	Gain a solid understanding of generative AI models, including large language models and text-to- image models
2	Utilize Lang Chain for developing advanced LLM applications and understand its components and functionalities
3	Develop practical skills in implementing chatbots, managing vector storage, and employing LLMs for data science.
4	Understand the principles of prompt engineering and learn how to design effective prompts for various AI applications.
5	Apply best practices in prompt engineering, address challenges, and incorporate ethical considerations in their work.

Sl. No	Title of the Book	Name of the Author/s	Name of the publisher	Edition & Year
Textbooks				
1	Generative AI with LangChain	Ben Auffarth	Packt Publishing Ltd.	1st Edition, 2023
2	Demystifying Prompt Engineering	Harish Bhat	Harish Bhat	1 st Edition, 2023
Reference Books				
1	"Generative Deep Learning: Teaching Machines to Paint, Write, Compose, and Play.	David Foster	O'Reilly Media	2nd Edition, 2023
2	Prompt Engineering for Generative AI: Future-Proof Inputs for Reliable AI Outputs	James Phoenix, Mike Taylor	O'Reilly Media	1 st Edition, 2024

Course Articulation Matrix (CO-PO and CO_PSO MAPPING)

Course Outcomes	Program Outcomes											PSOs		
	1	2	3	4	5	6	7	8	9	10	11	1	2	3
CO1	2											2		
CO2	2											2		
CO3		2											2	
CO4		2											2	
CO5		2											2	
Overall CO	2	2										2	2	

Program Articulation Matrix:

Course Outcomes	Program Outcomes											PSOs		
	1	2	3	4	5	6	7	8	9	10	11	1	2	3
	2	2										2	2	

Generative AI and Prompt Engineering Lab

Part A

1	Fine-Tuning GPT-2 for Domain-Specific Text Generation
2	Image-to-Image Translation with Stable Diffusion
3	LangChain-Powered Document QA System
4	Music Generation with Transformer Models
5	Multi-Modal Text-to-Image Synthesis
6	Custom Retriever for Domain-Specific Chatbots
7	Automated EDA with LLMs
8	Ethical AI - Bias Detection in Generated Text
9	Multi-Modal Voice-Enabled Chatbot
10	Time Series Forecasting with Autoformer
11	Multi-Lingual Chatbot with LangChain
12	Automated Data Cleaning with LLMs
13	Medical Report Generation with BioBERT
14	AI-Assisted Story Writing with Fine-Tuned GPT-Neo

Part B

1	Tone and Style Transfer via Prompts
2	Iterative Prompt Refinement for Creative Writing
3	Ethical Prompt Design for Bias Mitigation
4	Chain-of-Thought Prompting for Math Problems
5	Persona-Based Prompt Engineering
6	Automated Prompt Optimization with Genetic Algorithms

B.E. COMPUTER SCIENCE & ENGINEERING
(ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING)
 Outcome Based Education (OBE) and Choice Based Credit System (CBCS)
SEMESTER - VII

FEDERATED LEARNING

Contact Hours/ Week:	S7CI01	Credits:	50
Total Lecture Hours:	(3:2:0)	CIE Marks:	50
Course Code:		SEE Marks:	3
	42Hrs		28hrs

Course objectives:

This course will enable students to:

1.	Understand the foundational concepts of Federated Learning (FL).
2.	Explore the different FL architectures and algorithms.
3.	Learn privacy-preserving techniques and their implementation in FL
4.	Apply FL methods to real-world scenarios
5.	Evaluate and optimize FL models for performance and scalability.

UNIT I

(8 hours)

Introduction: Motivation, Federated Learning as a Solution, The Definition of Federated Learning, Categories of Federated Learning, Current Development in Federated Learning, Research Issues in Federated Learning, Open-Source Projects, Standardization Efforts, The Federated AI Ecosystem Background: Privacy-Preserving Machine Learning, PPML and Secure ML, Threat and Security Models, Privacy Threat Models, Adversary and Security Models, Privacy Preservation Techniques, Secure Multi-Party Computation, Homomorphic Encryption, Differential Privacy.

UNIT II

(8 hours)

Distributed Machine Learning: Introduction to DML, The Definition of DML, DML Platforms, Scalability-Motivated DML, Large-Scale Machine Learning, Scalability-Oriented DML Schemes, Privacy-Motivated DML, Privacy-Preserving Decision Trees, Privacy-Preserving Techniques, Privacy-Preserving DML Schemes, Privacy-Preserving Gradient Descent, Vanilla Federated Learning, Privacy-Preserving Methods.

UNIT III

(8 hours)

Horizontal Federated Learning: The Definition of HFL, Architecture of HFL, The Client- Server Architecture, The Peer-to-Peer Architecture, Global Model Evaluation, The Federated Averaging Algorithm, Federated Optimization, The FedAvg Algorithm, The Secured FedAvg Algorithm, Improvement of the FedAvg Algorithm, Communication Efficiency, Client Selection Vertical Federated Learning: The Definition of VFL, Architecture of VFL, Algorithms of VFL, Secure Federated Linear Regression, Secure Federated Tree-Boosting.

UNIT IV

(8 hours)

Federated Transfer Learning: Heterogeneous Federated Learning, Federated Transfer Learning, The FTL Framework, Additively Homomorphic Encryption, The FTL Training Process, The FTL Prediction Process, Security Analysis, Secret Sharing-Based FTL Incentive Mechanism Design for Federated Learning: Paying for Contributions, Profit-Sharing Games, Reverse Auctions, A Fairness-Aware Profit Sharing Framework, Modeling Contribution, Modeling Cost, Modeling Regret, Modeling Temporal Regret, The Policy Orchestrator, Computing Payoff Weightage.

UNIT V	(8 hours)
Federated Learning for Vision, Language, and Recommendation: Federated Learning for Computer Vision, Federated CV, Federated Learning for NLP, Federated NLP, Federated Learning for Recommendation Systems, Recommendation Model, Federated Recommendation System Federated Reinforcement Learning: Introduction to Reinforcement Learning, Policy, Reward, Value Function, Model of the Environment, RL Background Example, Reinforcement Learning Algorithms, Distributed Reinforcement Learning, Asynchronous Distributed Reinforcement Learning, Synchronous Distributed Reinforcement Learning, Federated Reinforcement Learning, Background and Categorization.	

Sl. No	Title of the Book	Name of the Author/s	Name of the publisher	Edition & Year
Textbooks				
1	Federated Learning: Privacy and Incentive	Qiang Yang, Yang Liu, Tianjian Chen, Yongxin Tong	Morgan & Claypool Publishers	2019
Reference Books				
1	Advances and Open Problems in Federated Learning	Peter Kairouz, H. Brendan McMahan,	arXiv:1912.04977	2019
2	Towards personalized federated learning.	Tan, A. Z., Yu, H., Cui, L., & Yang, Q.	<i>IEEE Transactions on Neural Networks and Learning Systems.</i>	2022
3	A survey on federated learning systems: Vision, hype and reality for data privacy and protection	Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., Li, Y	<i>IEEE Transactions on Knowledge and Data Engineering,</i>	2021

Practical Exercise List

Sl. No	Exercise
1	Centralized Training Baseline <ul style="list-style-type: none"> • Objective: Train a neural network on the MNIST dataset using centralized data. • Tasks: Load preprocess the MNIST dataset, Build and train a simple neural network, Evaluate model accuracy and loss.
2	Federated Learning with Flower: Getting Started <ul style="list-style-type: none"> • Objective: Convert centralized MNIST training to a federated setup. • Tasks: Split MNIST data across multiple simulated clients, Implement federated averaging (FedAvg) using Flower, Compare performance with centralized training.
3	Federated Learning with NVIDIA FLARE: Hello World <ul style="list-style-type: none"> • Objective: Set up a simple FL experiment using NVIDIA FLARE. • Tasks: Install NVFlare, Run the "Hello World" FL example, Observe client-server interaction and aggregation.
4	Exploring Federated Averaging (FedAvg) Algorithm <ul style="list-style-type: none"> • Objective: Deep dive into the FedAvg algorithm. • Tasks: Modify the Flower or NVFlare example to experiment with different client numbers and local epochs, Modify the Flower or NVFlare example to experiment with different client numbers and local epochs, Analyze convergence and communication efficiency.
5	Privacy-Preserving Techniques: Differential Privacy <ul style="list-style-type: none"> • Objective: Integrate differential privacy into FL.

	<ul style="list-style-type: none"> • Tasks: Add noise to model updates using Flower or NVFlare, Observe the impact on privacy and model accuracy.
6	Federated Proximal (FedProx) Algorithm <ul style="list-style-type: none"> • Objective: Implement and compare FedProx with FedAvg. • Tasks: Modify your FL setup to use the FedProx algorithm, Compare results on non-IID data distributions.
7	Vertical Federated Learning (VFL) Simulation <ul style="list-style-type: none"> • Objective: Simulate VFL where clients have different features of the same samples. • Tasks: Partition a dataset vertically (split features between two clients), Implement secure aggregation of model updates.
8	Federated Transfer Learning Objective: Apply transfer learning in a federated context. Tasks: Use pre-trained models as a starting point for FL, Fine-tune locally on client data and aggregate updates.
9	Application: Federated Learning for Medical Imaging Objective: Apply FL to a healthcare scenario. Tasks: Use the MedMNIST dataset, split across simulated hospitals, Train a federated model for image classification, Compare with centralized results.
10	Advanced: Communication Efficiency and Client Selection Objective: Explore strategies to reduce communication costs and select clients. Tasks: Implement periodic client selection, Experiment with model compression or quantization, Measure effects on training speed and accuracy.
Additional Open-Source FL Libraries <ul style="list-style-type: none"> • Flower: flower.ai • NVIDIA FLARE: github.com/NVIDIA/NVFlare • PFLlib: github.com/TsingZO/PFLlib • OpenFL: github.com/intel/openfl • Fed-BioMed: gitlab.inria.fr/fedbiomed 	

Course Articulation Matrix

Course Outcomes	Program Outcomes											PSOs		
	1	2	3	4	5	6	7	8	9	10	11	1	2	3
CO1	2	2	2									2	2	
CO2	2	2	2										2	
CO3	2	2												
CO4	2		2									2	2	
CO5	2	2										2	2	
Overall CO	2	2	2										2	2

Program Articulation Matrix:

Course Outcomes	Program Outcomes											PSOs		
	1	2	3	4	5	6	7	8	9	10	11	1	2	3
	2	2	2									2	2	2

B.E. COMPUTER SCIENCE & ENGINEERING
(ARTIFICIALINTELLIGENCE AND MACHINE LEARNING)
 Outcome Based Education (OBE) and Choice Based Credit System (CBCS)
SEMESTER - VII

EXPLAINABLE AND RESPONSIBLE AI

Course Code	S7CCSPE01	CIE Marks	50
Teaching Hours/Week (L:T:P)	(3:0:0)	SEE Marks	50
Credits	3	Exam Hours	3
Lecture Hours	28Hrs	Practical Hours	28Hrs

Course objectives: This course will enable students to:

1	Provide comprehensive understanding of Responsible AI and Explainable AI and its applications.
2	Explore key components of Responsible AI pattern catalogue.
3	Develop skills for building and implementing AI bots using LIME and SHAP tools.
4	Introduce the fundamentals and importance of developing responsible explainable AI agents.
5	Equip students with best practices and strategies for design and development of responsible AI architecture.

UNIT I

8 Hours

Introduction to Responsible AI: What Is Responsible AI?, What Is AI?, Developing AI Responsibly: Who Is Responsible for Putting the “Responsible” into AI?. Operationalizing Responsible AI: A Thought Experiment—Robbie the Robot, A Thought Experiment—Robbie the Robot, Who Should Be Involved in Building Robbie?, What Are the Responsible AI Principles for Robbie?, Robbie and Governance Considerations, Robbie and Process Considerations, Robbie and Product Considerations.

Overview of the Responsible AI Pattern Catalogue: The Key Concepts, the Multifaceted Meanings of Responsible, Varied Understandings of Operationalization, The Duality of Trust and Trustworthiness, Why Is Responsible AI Different?, A Pattern-Oriented Approach for Responsible AI

UNIT II

8 Hours

Pattern-Oriented Reference Architecture for Responsible-AI-by-Design: Architectural Principles for Designing AI Systems, Pattern-Oriented Reference Architecture, Supply Chain Layer, System Layer, Operation Infrastructure Layer.

Principle-Specific Techniques for Responsible AI: Fairness, Fairness Assessor, Discrimination Mitigator, Privacy, Encrypted-Data-Based Trainer, Secure Aggregator, Random Noise Data Generator, Explainability, Local Explainer, Global Explainer.

UNIT III

8 Hours

Process Patterns for Trustworthy Development Processes: Requirements: AI Suitability Assessment, Verifiable RAI Requirement, Lifecycle-Driven Data Requirement, RAI User Story, Design, Multi-Level Co-Architecting, Envisioning Card, RAI Design Modeling, System-Level RAI Simulation, XAI Interface, Implementation, RAI Governance of APIs, RAI Governance via APIs, RAI Construction with Reuse.

Testing, RAI Acceptance Testing, RAI Assessment for Test Cases, Operations, Continuous Deployment for RAI, Extensible, Adaptive, and Dynamic RAI Risk Assessment, Multi-Level Co-Versioning.

UNIT IV

8 Hours

An Overview of Explainability: What Are Explanations?, Explainability Consumers, Practitioners: Data Scientists and ML Engineers, Observers: Business Stakeholders & Regulators, End-Users: Domain Experts & Affected Users, Types of Explanations, Pre-modeling Explainability, Intrinsic vs. Post-Hoc Explainability, Local, Cohort, and Global Explanations, Attributions, Counterfactual, and Example-based, Themes Throughout Explainability, Feature Attributions, Surrogate Models, Activation

UNIT V	8 Hours
Explainability for Image Data: Integrated Gradients, Choosing a Baseline, Accumulating Gradients, Improvements on Integrated Gradients, XRAI, How XRAI works, Implementing XRAI, Grad-CAM, How Grad-CAM works, Implementing Grad-CAM, Improving Grad-CAM, LIME, How LIME Works, Implementing LIME, Guided Backpropagation and Guided Grad-CAM, Guided Backprop and DeConvNets, Guided Grad-CAM.	

Course Outcomes: On Successful completion of this course, students will be able to	
1	Gain a solid understanding of responsible and explainable AI.
2	Discuss the principle specific techniques for design of responsible AI considering fairness, security and privacy metrics.
3	Analyze the working process patterns for design and development of Trustworthy AI bots.
4	Illustrate the best practices for designing responsible and explainable AI bots for various societal applications with examples.
5	Utilize LIME and SHAP tools for developing responsible AI bots and understand its components and functionalities.

Sl. No	Title of the Book	Name of the Author/s	Name of the publisher	Edition & Year
Textbooks				
1	Responsible-AI: Best Practices for Creating-Trustworthy AI systems	Qinghua Lu, Liming Zhu, Jon Whittle, Xiwei Xu	Addison-Wesley Professional	Edition 1, 26 December 2023
2	Explainable AI for Practitioners	<u>Michael Munn, David Pitman</u>	O'Reilly Media, Inc.	Edition 1, October 2022
Reference Books				
1	Towards ethical and socially responsible explainable AI : challenges and oppurtunities	<u>Mohammad Amir, Khusru Akhtar , Mohit Kumar , Anand Nayyar</u>	Springer cham	Edition 1, August 2024
2	Explainable and Responsible Artificial Intelligence in Healthcare	<u>Rishabha, Malviya, Sonali , Sundram</u>	Wiley,	Edition 1, March 2025
3	Responsible AI in practice: A practical guide to safe and human AI	<u>Toju Duke , Paolo Giudici</u>	Apress Berkeley, CA	Edition 1, January 2025

Course Articulation Matrix (CO-PO and CO_PSO MAPPING)

Course Outcomes	Program Outcomes											PSOs			
	1	2	3	4	5	6	7	8	9	10	11	1	2	3	
CO1	2												2		
CO2		2											2		
CO3	2		2										2		
CO4			2		2								2		
CO5			2		2								2		
Overall CO	2	2	2		2								2		

Program Articulation Matrix:

Course Outcomes	Program Outcomes											PSOs			
	1	2	3	4	5	6	7	8	9	10	11	1	2	3	
	2	2	2		2								2		

B.E. COMPUTER SCIENCE & ENGINEERING (ARTIFICIALINTELLIGENCE AND MACHINE LEARNING) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER - VII			
ROBOTIC PROCESS AUTOMATION			
Course Code	S7CCSPE02	CIE Marks	50
Teaching Hours/Week (L:T:P)	(3:0:0)	SEE Marks	50
Credits	3	Exam Hours	3
Lecture Hours	42Hrs	Practical Hours	-

Course objectives: This course will enable students to:	
1	To understand basic concepts of RPA
2	To Describe RPA, where it can be applied and how it implemented
3	To Describe the different types of variables, Control Flow and data manipulation techniques
4	To Understand Image, Text and Data Tables Automation
5	To Describe various types of Exceptions and strategies to handle

UNIT I	9 Hours
RPA Foundations- What is RPA - Flavours of RPA- History of RPA- The Benefits of RPA- The downsides of RPA- RPA Compared to BPO, BPM and BPA - Consumer Willingness for Automation- The Workforce of the Future- RPA Skills-On-Premise Vs. the Cloud- Web Technology- Programming Languages and Low Code-OCR-Databases-APIs- AI-Cognitive Automation-Agile, Scrum, Kanban and Waterfall, Devops- Flowcharts. Textbook 1: Ch 1, Ch 2	

UNIT II	8 Hours
RPA Platforms- Components of RPA- RPA Platforms-About Ui Path- About UiPath - The future of automation - Record and Play - Downloading and installing UiPath Studio -Learning Ui Path Studio- - Task recorder - Step-by-step, Examples using the recorder. Textbook 2= Ch 1, Ch 2	

UNIT III	9 Hours
Sequence, Flowchart, and Control Flow- Sequencing the workflow- Activities-Control flow, various types of loops, and decision making-Step-by-step example using Sequence and Flowchart-Step-by-step example using Sequence and Control Flow-Data Manipulation-Variables and Scope- Collections-Arguments - Purpose and use-Data table usage with examples- Clipboard management-File operation with step-by-step example-CSV/Excel to data table and vice versa (with a step-by-step example). Textbook 2: Ch 3, Ch 4	

UNIT IV	8 Hours
Taking Control of the Controls- Finding and attaching windows- Finding the control- Techniques for waiting for a control- Act on controls - mouse and keyboard activities- Working with UiHxplorer- Handling events- Revisit recorder- Screen Scraping- When to use OCR- Types of OCR available- How to use OCR- Avoiding typical failure points. Textbook 2: Ch 5	

UNIT V	8 Hours
Exception Handling, Debugging, and Logging- Exception handling- Common exceptions and ways to handle them- Logging and taking screenshots-Debugging techniques- Collecting crash dumps- Error reporting- Future of RPA. Text book 1: Ch 13, Text book 2: Ch 8	

Course Outcomes: On Successful completion of this course, students will be able to	
1	Understand the basic concepts of RPA
2	Describe various components and platforms of RPA

3	Describe the different types of variables, control flow and data manipulation techniques
4	Understand various control techniques and OCR in RPA
5	Describe various types and strategies to handle exceptions

Sl. No	Title of the Book	Name of the Author/s	Name of the publisher	Edition & Year
Textbooks				
1	The Robotic Process Automation Handbook: A Guide to Implementing RPA Systems	Tom Taulli	A press	2020,ISBN-13 (electronic):978-7-4842-5729-6
2	Learning Robotic Process Automation,	Alok Mani Tripathi,	Packt Publishing	March 2018 ISBN: 9787788470940
Reference Books				
1	Introduction to Robotic Process Automation: a Primer	Frank Casale, Rebecca Dilla, Iieidi Jaynes, Lauren Livingston	Institute of Robotic Process Automation.	
2	Robotic Process Automation: Guide To Building Software Robots, Automate Repetitive Tasks & Become An RPA Consultant	Richard Murdoch	Computer Bookshop (I) Pvt. Ltd.	ISBN-13 : 978-1983036835
3	Robotic Process Automation Tools, Process Automation and their benefits: Understanding RPA and Intelligent Automation	Srikanth Merianda	Createspace Independent Publishing Platform (26 May 2018)	2018, ISBN-13 : 978-1720626077

Course Articulation Matrix (CO-PO and CO_PSO MAPPING)

Course Outcomes	Program Outcomes											PSOs			
	1	2	3	4	5	6	7	8	9	10	11	1	2	3	
CO1	3														
CO2		2											2		
CO3			2												
CO4			2												
CO5					2										
Overall CO	3	2	2		2								2		

Program Articulation Matrix:

Course Outcomes	Program Outcomes											PSOs			
	1	2	3	4	5	6	7	8	9	10	11	1	2	3	
	3	2	2		2								2		

B.E. COMPUTER SCIENCE & ENGINEERING
(ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING)
 Outcome Based Education (OBE) and Choice Based Credit System (CBCS)
SEMESTER - VII

AGENTIC AI – FOUNDATIONS AND APPLICATIONS

Course Code	S7CCSPE03	CIE Marks	50
Teaching Hours/Week (L:T:P)	(3:0:0)	SEE Marks	50
Credits	3	Exam Hours	3
Lecture Hours	42Hrs	Practical Hours	-

Course objectives: This course will enable students to:

1	Understand the foundations and evolution of agentic AI and its differences from traditional AI.
2	Learn agent architectures and environmental characteristics for effective agent system design.
3	Analyze and implement communication and coordination strategies in multi-agent systems.
4	Understand learning paradigms in agentic AI to design adaptive agents.
5	Familiarize with ethical, security, and technological challenges in advanced agentic AI.

UNIT I

(9 Hours)

Introduction to Agentic AI

- 1.1 : **Foundations of AI**
 - 1.1.1 : History and Evolution of AI (References: T1: Ch.1, Sec.1.2; R1: Ch.1, Sec.1.1; W1)
 - 1.1.2 : Definitions and Approaches to AI (References: T1: Ch.1, Sec.1.1; R1: Ch.1, Sec.1.2; W2)
- 1.2 : **Agent Paradigm**
 - 1.2.1 : Definition of an Agent (References: T1: Ch.2, Sec.2.1; T2: Ch.2, Sec.2.1; W3)
 - 1.2.2 : Types of Agents (References: T1: Ch.2, Sec.2.4; T2: Ch.2, Sec.2.2; W4)
- 1.3 : **Agentic AI vs Traditional AI**
 - 1.3.1 : Autonomy and Proactivity (References: T1: Ch.2, Sec.2.3; T2: Ch.2, Sec.2.3; W5)
 - 1.3.2 : Goal-Directed Behaviour (References: T1: Ch.2, Sec.2.4.3; T2: Ch.2, Sec.2.4; W6)
- 1.4 : **Applications of Agentic AI**
 - 1.4.1 : Real-world Examples (References: T1: Ch.1, Sec.1.4; T2: Ch.1, Sec.1.2; W7)

UNIT II

(9 Hours)

Agent Architectures and Environments

- 2.1 : **Agent Architectures**
 - 2.1.1 : Simple Reflex Agents (References: T1: Ch.2, Sec.2.4.1; T2: Ch.2, Sec.2.2; W8)
 - 2.1.2 : Model-based Reflex Agents (References: T1: Ch.2, Sec.2.4.2; T2: Ch.2, Sec.2.2; W9)
 - 2.1.3 : Goal-based Agents (References: T1: Ch.2, Sec.2.4.3; T2: Ch.2, Sec.2.2; W10)
 - 2.1.4 : Utility-based Agents (References: T1: Ch.2, Sec.2.4.4; T2: Ch.2, Sec.2.2; W11)
 - 2.1.5 : Learning Agents (References: T1: Ch.2, Sec.2.4.5; T2: Ch.2, Sec.2.2; W12)
- 2.2 : **Environments for Agents**
 - 2.2.1 : Properties of Environments (References: T1: Ch.2, Sec.2.3; T2: Ch.2, Sec.2.3; W13)
 - 2.2.2 : Environment Types (PEAS) (References: T1: Ch.2, Sec.2.3; T2: Ch.2, Sec.2.3; W14)
 - 2.2.3 : Environment Modeling (References: T1: Ch.2, Sec.2.3; R1: Ch.2, Sec.2.2; W15)

UNIT III

(8 Hours)

Agent Communication and Coordination

- 3.1 : **Agent Communication**
 - 3.1.1 : Communication Languages (References: T2: Ch.6, Sec.6.2; R1: Ch.13, Sec.13.2; W16)
 - 3.1.2 : Speech Acts and Semantics (References: T2: Ch.6, Sec.6.3; R1: Ch.13, Sec.13.3; W17)
 - 3.1.3 : Agent Communication Protocols (References: T2: Ch.6, Sec.6.4; R1: Ch.13, Sec.13.4; W18)
- 3.2 : **Coordination in Multi-Agent Systems**
 - 3.2.1 : Coordination Strategies (References: T2: Ch.7, Sec.7.1; R1: Ch.13, Sec.13.5; W19)
 - 3.2.2 : Distributed Problem Solving (References: T2: Ch.7, Sec.7.2; R1: Ch.13, Sec.13.6; W20)
 - 3.2.3 : Negotiation and Conflict Resolution (References: T2: Ch.7, Sec.7.3; R1: Ch.13, Sec.13.7; W21)
- 3.3 : **Applications of Agent Communication and Coordination**
 - 3.3.1 : Real-world Multi-Agent Systems (References: T2: Ch.1, Sec.1.2; R1: Ch.1, Sec.1.3; W22)

UNIT IV		(8 Hours)
Learning in Agentic AI		
4.1	: Introduction to Learning in Agents	
4.1.1	: Need for Learning in Agents (References: T1: Ch.2, Sec.2.4.5; R1: Ch.20, Sec.20.1; W23)	
4.1.2	: Types of Learning (References: T1: Ch.18, Sec.18.1; R1: Ch.20, Sec.20.2; W24)	
4.2	: Supervised and Unsupervised Learning	
4.2.1	: Supervised Learning (References: T1: Ch.18, Sec.18.2; R1: Ch.20, Sec.20.3; W25)	
4.2.2	: Unsupervised Learning (References: T1: Ch.18, Sec.18.3; R1: Ch.20, Sec.20.4; W26)	
4.3	: Reinforcement Learning	
4.3.1	: Reinforcement Learning Basics (References: T1: Ch.21, Sec.21.1; R1: Ch.21, Sec.21.1; W27)	
4.3.2	: Q-Learning and Policy Learning (References: T1: Ch.21, Sec.21.3; R1: Ch.21, Sec.21.2; W28)	
4.4	: Integration of Learning in Agent Architectures	
4.4.1	: Learning Agents (References: T1: Ch.2, Sec.2.4.5; T2: Ch.2, Sec.2.2; W29)	
4.4.2	: Applications of Learning Agents (References: T1: Ch.25, Sec.25.1; T2: Ch.1, Sec.1.2; W30)	

UNIT V		(8 Hours)
Advanced Topics in Agentic AI		
5.1	: Ethical and Social Issues	
5.1.1	: Ethics in Agentic AI (References: T1: Ch.27, Sec.27.1; R1: Ch.26, Sec.26.1; W31)	
5.1.2	: Social Impact and Responsibility (References: T1: Ch.27, Sec.27.2; R1: Ch.26, Sec.26.2; W32)	
5.2	: Explainability and Transparency	
5.2.1	: Explainable Agentic Systems (References: T1: Ch.27, Sec.27.3; R1: Ch.26, Sec.26.3; W33)	
5.2.2	: Human-Agent Interaction (References: T1: Ch.27, Sec.27.4; T2: Ch.10, Sec.10.2; W34)	
5.3	: Security and Robustness	
5.3.1	: Security Challenges in Agentic AI (References: T1: Ch.27, Sec.27.5; R1: Ch.26, Sec.26.4; W35)	
5.3.2	: Robustness and Safety (References: T1: Ch.27, Sec.27.6; R1: Ch.26, Sec.26.5; W36)	
5.4	: Integration with Emerging Technologies	
5.4.1	: Agentic AI and IoT (References: T1: Ch.25, Sec.25.3; T2: Ch.11, Sec.11.2; W37)	
5.4.2	: Agentic AI in Cloud and Edge Computing (References: T1: Ch.25, Sec.25.4; T2: Ch.11, Sec.11.3; W38)	
5.5	: Future Directions	
5.5.1	: Research Trends in Agentic AI (References: T1: Ch.28, Sec.28.1; R1: Ch.27, Sec.27.1; W39)	
5.5.2	: Open Challenges (References: T1: Ch.28, Sec.28.2; R1: Ch.27, Sec.27.2; W40)	

Course Outcomes: On Successful completion of this course, students will be able to	
1	Explain the foundational concepts and evolution of agentic artificial intelligence.
2	Identify and design appropriate agent architectures and model agent environments.
3	Implement communication and coordination strategies in multi-agent systems.
4	Apply learning algorithms to develop adaptive and intelligent agents.
5	Analyze and address ethical, security, and technological challenges in advanced agentic AI applications.

Sl. No	Title of the Book	Name of the Author/s	Name of the publisher	Edition & Year
Textbooks				
1	Artificial Intelligence: A Modern Approach	Stuart Russell, Peter Norvig	Pearson	4th, 2021
2	An Introduction to MultiAgent Systems	Michael Wooldridge	Wiley	4th, 2021
Reference Books				
1	Artificial Intelligence: Foundations of Computational Agents	David Poole, Alan Mackworth	Cambridge University Press	2nd,2017

Course Articulation Matrix (CO-PO and CO_PSO MAPPING)

Course Outcomes	Program Outcomes											PSOs			
	1	2	3	4	5	6	7	8	9	10	11	1	2	3	
CO1	2		2										2		
CO2			2										2		
CO3			2										2		
CO4			2										2		
CO5	2		2										2		
Overall CO	2		2										2		

Program Articulation Matrix:

Course Outcomes	Program Outcomes											PSOs			
	1	2	3	4	5	6	7	8	9	10	11	1	2	3	
	2		2										2		

B.E. COMPUTER SCIENCE & ENGINEERING
(ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING)
 Outcome Based Education (OBE) and Choice Based Credit System (CBCS)
SEMESTER - VII

AI IN DATA SECURITY & PRIVACY

Course Code	S7CCSPE04	CIE Marks	50
Teaching Hours/Week (L:T:P)	(3:0:0)	SEE Marks	50
Credits	3	Exam Hours	3
Lecture Hours	42Hrs	Practical Hours	-

Course objectives: This course will enable students to:

1	Equip with a deep understanding of the evolving data ecosystem, the ethical and security challenges posed by AI-driven data management
2	Analyze real-world AI incidents, understand the security and ethical challenges of automation and smart city technologies
3	Comprehensive understanding of foundational and emerging cybersecurity strategies
4	Gain the knowledge and tools necessary to manage technological, operational, and strategic risks associated with AI systems through comprehensive assessment, mitigation, and communication strategies.
5	Leverage AI-driven technologies for real-time threat monitoring, predictive analysis, automated detection, and effective incident response in modern cybersecurity environments

UNIT I

8 Hours

Introduction: The New Data Landscape, The Role of AI in Modern Data Management, The Digital Imprint, The Confluence of Data Streams, From Data Points to Personal Stories, The Illusion of Anonymity in Big Data, The Ethical Dilemmas of Predictive Analytics, The Double-edged Sword of Personalization, Data Sovereignty in a Borderless Digital World, The Imperative of Data Protection, AI-driven Data Governance, Democratizing Data Management,

Understanding the AI Threat Landscape: The Rise of Rogue AI, The Intricate Foundations of AI Learning, Biases: The Unseen Puppeteers, Deepfakes: The Erosion of Trust, Physical Manifestations: A Tangible Threat, How AI Can Exploit Data Gaps, Unraveling the Complexity of Data Gaps. The Inherent Nature of AI to Compensate, Rogue Elements and Their Advantage, The Perils of Unbridled Faith in AI

UNIT II

8 Hours

Case Study: The Impact of AI Bias in Healthcare Diagnostics, Background, The Incident, Investigation and Findings, Consequences, Resolution and Lessons Learned, Conclusion

Smart Cities: A Vision Marred by Data Gaps, Real-World AI Data Breaches: Lessons Learned, The Notorious Chatbot Incident, The Health Data Exposure, Autonomous Vehicles: When AI Meets the Real World, Lessons Drawn, Double-Edged Sword of Automation and Citizen Development Tools, Introduction to Automation Risks, RPA: Efficiency versus Security Trade-offs, Low-Code/No-Code Platforms: Democratization versus Compliance, Challenges of Automation in Smart Cities, Lessons and Strategies for Mitigation

Data Classification and Management: Defining Sensitive Data in the AI Era, AI-Driven Data Classification Techniques, Lifecycle of Data: Creation to Destruction, Role of Metadata in Classification, Ethical Considerations in AI-Driven Data Classification, Adaptive Data Classification, Role of Privacy-Preserving AI in Data Management, Data Classification Tools, Empowering Citizen Developers

UNIT III

8 Hours

Foundations of AI-Proof Security: Role of Encryption: Traditional versus Quantum, Multi-factor Authentication (MFA) and Biometrics, Blockchain: The Immutable Data Keeper, The Importance of Zero-Trust Architecture, Behavioral Analytics and AI-Powered Threat Detection, Secure Software Development Lifecycle (SSDLC), AI-Powered Penetration Testing, Red Teaming and AI Simulations, Data Masking and Anonymization, Container Security and AI-Driven Vulnerability Management, The Power of Sandboxing in AI-Powered Security, Security Informaion and Event Management (SIEM) in the AI Era.

UNIT IV	8 Hours
<p>AI Risk Management: Understanding AI Risk, Types and Consequences, Technological Risks, Operational Risks, Strategic Risks, Risk Assessment in AI Systems, Understanding the Landscape, Probing the Shadows for Threats, Vulnerability: AI's Achilles' Heel, Quantifying the Consequences, AI Risk Mitigation Strategies, Contextual Security Measures, Robust Data Management, System Transparency and Interpretability, Tailored AI Monitoring Systems, Adaptive Security Protocols, Collaborative Threat Intelligence, AI Risk Communication and Reporting, Incident Notification Protocols, Maintaining Transparency with Stakeholders, Post-Incident Analysis and Learning, Real-World Examples of Risk Communication, Ongoing Review and Updates to AI Risk Management, Scheduled Risk Assessment Revisions, Incorporating New Threat Intelligence, Engaging with AI Security Communities</p>	
<p>Advanced AI-Proof Data Storage Solutions: Quantum-resistant Cryptography, The Advent of Quantum Computing, Post-quantum Cryptographic Algorithms, Transitioning from Classical to Quantum-Resistant Security, The Future of Quantum-resistant Cryptography.</p>	

UNIT V	8 Hours
<p>Monitoring, Detection, and Response: AI in Threat Intelligence, Predictive Analysis: Forecasting Cyber Threats, Phishing Detection: Automating the Identification Process, Dark Web Monitoring: Keeping Tabs on the Underbelly of the Internet, Automated Threat Ranking: Prioritizing Threats for Effective Response, Real-time Monitoring and Anomaly Detection, Behavioral Analysis: Understanding User Patterns, Network Traffic Insights: Monitoring Data Flow, Endpoint Security: Keeping Devices Safe in Real-time, AI-powered Intrusion Detection Systems: Advanced Threat Recognition, Incident Response in an AI-Driven World, Automated Responses: Swift Action Against Threats, Human-AI Collaboration: Merging Intuition with Algorithms, Post-Incident Analysis: Learning from Breaches Using AI, AI in Digital Forensics: Unraveling Complex Cyber Crimes.</p>	

Course Outcomes: On Successful completion of this course, students will be able to	
1	Critically evaluate the ethical, societal, and technical implications of AI in data management,
2	Apply ethical, secure, and inclusive AI-driven data management practices across various sectors
3	Comprehensive knowledge and practical skills to implement resilient, AI-aware cybersecurity strategies using modern technologies
4	Acquire the skills to effectively identify, assess, mitigate, and communicate AI-related risks to ensure secure, transparent, and resilient AI system deployment
5	Implement AI-powered tools and techniques for real-time threat detection, automated response, and post-incident analysis to enhance cybersecurity resilience.

Sl. No	Title of the Book	Name of the Author/s	Name of the publisher	Edition & Year
Textbooks				
1	AI Data Privacy and Protection: AI Data Privacy and Protection	Technics Publications	Technics Publications	2024
Reference Books				
1	Handbook on Data Protection and Privacy for Developers of Artificial Intelligence (AI) in India: Practical Guidelines for Responsible Development of AI	Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH.	KOAN Advisory (Varun Ramdas, Priyesh Mishra, Aditi Chaturvedi) Digital India Foundation (Nipun Jain)	July 2021
2	Data Security and Privacy Protection, A Comprehensive Guide, World Scientific Connect	<u>Anyu Wang</u> (<i>Cloud Security Alliance Great China Region, China</i>)	World Scientific	April 2025

B.E. COMPUTER SCIENCE & ENGINEERING
(ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING)
 Outcome Based Education (OBE) and Choice Based Credit System (CBCS)
SEMESTER - VII

BLOCKCHAIN TRACED AI

Course Code	S7CCSPE05	CIE Marks	50
Teaching Hours/Week (L:T:P)	(3:0:0)	SEE Marks	50
Credits	3	Exam Hours	3
Lecture Hours	42Hrs	Practical Hours	-

Course objectives: This course will enable students to:

1	Comprehend the fundamentals of Blockchain and its organization.
2	Analyse the underlying concepts of working of a Blockchain.
3	Study the working principles of Bitcoin.
4	Demonstrate the working of Blockchain using Ethereum.
5	Examine and explore possible business applications of Blockchain.

UNIT I

9 Hours

Introduction to Blockchain, Backstory of Blockchain, What is Blockchain?, Centralized vs. Decentralized Systems, Centralized Systems, Decentralized Systems, Layers of Blockchain, Application Layer, Execution Layer, Semantic Layer, Propagation Layer, Consensus Layer, Why is Blockchain Important?, Limitations of Centralized Systems, Blockchain Adoption So Far, Blockchain Uses and Use Cases

T1 – Chapter 1

How Blockchain Works: Laying the Blockchain Foundation, Cryptography: Symmetric Key Cryptography, Cryptographic Hash Functions, MAC and HMAC, Asymmetric Key Cryptography, Diffie-Hellman Key Exchange, Symmetric vs. Asymmetric Key Cryptography.

T1 – Chapter 2

UNIT II

9 Hours

Why Build a Blockchain Truth Machine for AI: Dissecting AI's Trust Deficit, Machine Learning Concerns, Black Box Algorithms, Genetic Algorithms, Data Quality, Outliers, and Edge Cases, Supervised Versus Unsupervised ML, Reinforcement Learning and Deep Learning, Program Synthesis, Superintelligent Agents, Technological Singularity, Attacks and Failures, Model/Data Drift, Adversarial Data Attacks, Risk and Liability, Blockchain as an AI Tether.

Enterprise Blockchain, Distributed, Linked Blocks, Trust and Transparency, Defining Your Use Case, Audit Trail, Local Memory Bank, Shared Memory Bank, Four Controls, Case Study: Oracle AIoT and Blockchain

T2 – Chapter 1

UNIT III

8 Hours

Blockchain Controls for AI: Four Blockchain Controls,
 Blockchain Control 1: Pre-establishing Identity and Workflow Criteria for People and Systems
 Blockchain Control 2: Distributing Tamper-Evident Verification
 Blockchain Control 3: Governing, Instructing, and Inhibiting Intelligent Agents
 Blockchain Control 4: Showing Authenticity Through User-Viewable Provenance

T2 – Chapter 2

UNIT IV

8 Hours

User Interfaces: Design Thinking: Web Interfaces, Blockchain Tethered AI User Interfaces, BTA User Mockups, Functionality, Traceability and Transparency, Smartphone and Tablet Apps, Email and Text Notifications, Spreadsheets.

Third-Party Systems: Working with APIs, Integrated Hardware, Third-Party Services and Tools

System Security: AI Security, Database Security, Blockchain Security, Additional Security.

T2 – Chapter 3

Planning Your BTA: BTA Architecture, Sample Model, AI Factsheet: Traffic Signs Detection Model, How the Model Works, Tethering the Model, Subscribing, Controlling Access: Organization Units, Staffings,

Users, Analyzing the Use Case: Participants, Assets, Transactions, Smart Contracts, Audit Trail
T2 – Chapter 4

UNIT V

8 Hours

Preparing for Development: Model, Installation, Bucket, Setting up Blockchain network, Install, Configure, and Launch the Blockchain, BTA- Front end and Backend, Test Your Environment, to begin building the application.
T2 – Chapter 5,6

Course Outcomes: On Successful completion of this course, students will be able to

1.	Describe the concepts of Blockchain and its structure.
2.	Outline the prerequisite concepts of Blockchain.
3.	Illustrate the working of Bitcoin cryptocurrency.
4.	Demonstrate the concepts of Blockchain on Ethereum platform for a suitable application.
5.	Examine potential business use cases of Blockchain

Sl. No	Title of the Book	Name of the Author/s	Name of the publisher	Edition & Year
Textbooks				
1	Beginning Blockchain	Bikramaditya Singhal, Gautam Dhameja, Priyansu Sekhar Panda	Apress Media	2018, ISBN 9781484234433
2	Blockchain for Dummies	Manav Gupta	John Wiley & Sons	2nd IBM Limited Edition, ISBN 9781119545934
Reference Books				
1	Blockchain for Business 2019	Peter Lypovonyav	Packt Publishing Limited	2019, ISBN 9781789956023
2	Ethereum for Architects and Developers	Debajani Mohanty	Apress Media	2018, ISBN 9781484240748
3	Regulating Blockchain Techno-Social and Legal Challenges	Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos, and Stefan Eich	Oxford University Press	2019, ISBN: 9780198842187

Course Articulation Matrix (CO-PO and CO_PSO MAPPING)

Course Outcomes	Program Outcomes											PSOs			
	1	2	3	4	5	6	7	8	9	10	11	1	2	3	
CO1	2												2		
CO2	2												2		
CO3	2												2		
CO4			2		2								2		
CO5		2											2		
Overall CO	2	2	2		2								2		

Program Articulation Matrix:

Course Outcomes	Program Outcomes											PSOs		
	1	2	3	4	5	6	7	8	9	10	11	1	2	3
	2	2	2									2	2	3

Human Computer Interactions

Duration :	12 weeks
Category :	Computer Science and Engineering

Course layout

Week 1: Introduction to HCI + Case study

Week 2: What is Design + Case study

Week 3: What is Interaction + Case study

Week 4: What is the User Perspective + Case study

Week 5: What is an Interface + Case study

Week 6: What is Data Requirement, Gathering and Analysis

Week 7: Prototyping and Smart UI + Case study

Week 8: Iterative Design and Evaluation + Case study

Week 9: HCI with IoT and Applications + Case study

Week 10: HCI and AI (including LLMs) + Case study

Week 11: Privacy, Security, and HCI + Case study

Week 12: HCI and AI based Conversational Systems and Applications(e.g., Finance, Healthcare, Education, Software Engineering, Assessment, Information Retrieval) + Projects

Foundations of Cyber Physical Systems

Duration :	12 weeks
Category :	Computer Science and Engineering

Course layout

Week 1: CPS : Motivational examples and compute platforms

Week 2: Real time sensing and communication for CPS

Week 3: Real time task scheduling for CPS

Week 4: Dynamical system modeling, stability, controller design

Week 5: Delay-aware Design; Platform effect on Stability/Performance

Week 6: Hybrid Automata based modeling of CPS

Week 7: Reachability analysis

Week 8: Lyapunov Stability, Barrier Functions

Week 9: Quadratic Program based safe Controller Design

Week 10: Neural Network (NN) Based controllers in CPS

Week 11: State Estimation using Kalman Filters (KF)

Week 12: Attack Detection and Mitigation in CPS

GPU Architectures and Programming

Duration :	12 weeks
Category :	Computer Science and Engineering

Course layout

Week 1 :Review of Traditional Computer Architecture – Basic five stage RISC Pipeline, Cache Memory, Register File, SIMD instructions

Week 2 :GPU architectures - Streaming Multi Processors, Cache Hierarchy, The Graphics Pipeline

Week 3 :Introduction to CUDA programming

Week 4 :Multi-dimensional mapping of dataspace, Synchronization

Week 5 :Warp Scheduling, Divergence

Week 6 :Memory Access Coalescing

Week 7 :Optimization examples : optimizing Reduction Kernels

Week 8 :Optimization examples : Kernel Fusion, Thread and Block

Week 9 :OpenCL basics

Week 10 :OpenCL for Heterogeneous Computing

Week 11-12 :Application Design : Efficient Neural Network Training/Inferencing

Cryptography and Network Security

Duration :	12 weeks
Category :	Computer Science and Engineering Systems

Course layout

Week 1: Introduction to cryptography, Classical Cryptosystem, Block Cipher.

Week 2: Data Encryption Standard (DES), Triple DES, Modes of Operation, Stream Cipher.

Week 3: LFSR based Stream Cipher, Mathematical background, Abstract algebra, Number Theory.

Week 4: Modular Inverse, Extended Euclid Algorithm, Fermat's Little Theorem, Euler Phi-Function, Euler's theorem.

Week 5: Advanced Encryption Standard (AES), Introduction to Public Key Cryptosystem, Diffie-Hellman Key Exchange, Knapsack Cryptosystem, RSA Cryptosystem.

Week 6: Primarily Testing, ElGamal Cryptosystem, Elliptic Curve over the Reals, Elliptic curve Modulo a Prime.

Week 7: Generalized ElGamal Public Key Cryptosystem, Rabin Cryptosystem.

Week 8 : Message Authentication, Digital Signature, Key Management, Key Exchange, Hash Function.

Week 9 : Cryptographic Hash Function, Secure Hash Algorithm (SHA), Digital Signature Standard (DSS).

Week 10: Cryptanalysis, Time-Memory Trade-off Attack, Differential and Linear Cryptanalysis.

Week 11: Cryptanalysis on Stream Cipher, Modern Stream Ciphers, Shamir's secret sharing and BE, Identity-based Encryption (IBE), Attribute-based Encryption (ABE).

Week 12: Side-channel attack, The Secure Sockets Layer (SSL), Pretty Good Privacy (PGP), Introduction to Quantum Cryptography, Blockchain, Bitcoin and Cryptocurrency.

Affective Computing

Duration :	12 weeks
Category :	Computer Science and Engineering Artificial Intelligence

Course layout

Week 1: Fundamentals of Affective Computing

Week 2: Emotion Theory and Emotional Design

Week 3: Experimental Design: Affect Elicitation; Research and Development Tools

Week 4: Emotions in Facial Expressions

Week 5: Emotions in Voice

Week 6: Emotions in Text

Week 7: Emotions in Physiological Signals

Week 8: Multimodal Emotion Recognition

Week 9: Emotional Empathy in Agents/Machines/Robots

Week 10: Online and Adaptive Recognition of Emotions: Challenges and Opportunities

Week 11: Case Study: Updated from Time to Time

Week 12: Ethical Issues: Ethical, legal and Social Implications of Affective Computing

Privacy and Security in Online Social Media

Duration :	12 weeks
Category :	Computer Science and Engineering Cyber Security

Course layout

Week 1: What is Online Social Networks, data collection from social networks, challenges, opportunities, and pitfalls in online social networks, APIs

Week 2: Collecting data from Online Social Media.

Week 3: Trust, credibility, and reputations in social systems

Week 4: Trust, credibility, and reputations in social systems

Week 5: Online social Media and Policing

Week 6: Information privacy disclosure, revelation and its effects in OSM and online social networks

Week 7: Phishing in OSM & Identifying fraudulent entities in online social networks

Week 8: Refresher for all topics

Week 9 to 12: Research paper discussion

Introduction to Industry 4.0 and Industrial Internet of Things

Duration :	12 weeks
Category :	Computer Science and Engineering

Course layout

Week 1 : Introduction: Sensing & actuation, Communication-Part I, Part II, Networking-Part I, Part II

Week 2 : Industry 4.0: Globalization and Emerging Issues, The Fourth Revolution, LEAN Production Systems, Smart and Connected Business Perspective, Smart Factories

Week 3 : Industry 4.0: Cyber Physical Systems and Next Generation Sensors, Collaborative Platform and Product Lifecycle Management, Augmented Reality and Virtual Reality, Artificial Intelligence, Big Data and Advanced Analysis

Week 4 : Cybersecurity in Industry 4.0, Basics of Industrial IoT: Industrial Processes-Part I, Part II, Industrial Sensing & Actuation, Industrial Internet Systems.

Week 5 : IIoT-Introduction, Industrial IoT: Business Model and Reference Architecture: IIoT-Business Models-Part I, Part II, IIoT Reference Architecture-Part I, Part II.

Week 6 : Industrial IoT- Layers: IIoT Sensing-Part I, Part II, IIoT Processing-Part I, Part II, IIoT Communication-Part I.

Week 7 : Industrial IoT- Layers: IIoT Communication-Part II, Part III, IIoT Networking-Part I, Part II, Part III.

Week 8 : Industrial IoT: Big Data Analytics and Software Defined Networks: IIoT Analytics - Introduction, Machine Learning and Data Science - Part I, Part II, R and Julia Programming, Data Management with Hadoop.

Week 9 : Industrial IoT: Big Data Analytics and Software Defined Networks: SDN in IIoT-Part I, Part II, Data Center Networks, Industrial IoT: Security and Fog Computing: Cloud Computing in IIoT-Part I, Part II.

Week 10 : Industrial IoT: Security and Fog Computing - Fog Computing in IIoT, Security in IIoT-Part I, Part II, Industrial IoT- Application Domains: Factories and Assembly Line, Food Industry.

Week 11 : Industrial IoT- Application Domains: Healthcare, Power Plants, Inventory Management & Quality Control, Plant Safety and Security (Including AR and VR safety applications), Facility Management.

Week 12 : Industrial IoT- Application Domains: Oil, chemical and pharmaceutical industry, Applications of UAVs in Industries, Real case studies :

Case study - I : Milk Processing and Packaging Industries

Case study - II: Manufacturing Industries - Part I

Case study - III : Manufacturing Industries - Part II

Case study - IV : Student Projects - Part I

Case study - V : Student Projects - Part II

Case study - VI : Virtual Reality Lab

Case study - VII : Steel Technology Lab

Responsible and Safe AI Systems

Duration :	12 weeks
Category :	Computer Science and Engineering Artificial Intelligence

Course layout

Week 1 & 2:

AI Capabilities Improvement in last 5-10 years

- Imminent risks from AI Models: Toxicity, bias, goal misspecification, adversarial examples etc.
- Long-term risks from AI Models: Misuse, Misgeneralization, Rogue AGI
- Principles of RAI - Transparency; Accountability; Safety, Robustness and Reliability; Privacy and Security; Fairness and non-discrimination; Human-Centred Values; Inclusive and Sustainable development, Interpretability
- Recap of Deep Learning Techniques, Language/Vision Models
- AI Risks for Gen models
- Adversarial Attacks – Vision, NLP, Superhuman Go agents

Week 3 & 4:

ML Poisoning Attacks like Trojans

- Implications for current and future AI safety
- Explainability
- Imminent and Long-term potential for transparency techniques
- Mechanistic Interpretability
- Representation Engineering, model editing and probing
- Critiques of Transparency for AI Safety

Week 5 & 6:

- Privacy & Fairness in AI

Week 7 & 8:

- Metrics and Tools for RAI - measuring bias/fairness, adversarial testing, explanations (Lime/SHAP/GradCam), audit mechanisms

- Regulation landscape - DPDP act (India), GDPR (EU), EU AI act, US presidential declaration, Ethical approvals, informed consent, participatory design, future of work, Indian context
- What is AGI? When could it be achieved?
- Instrumental Convergence: Power Seeking, Deception etc.

Week 9 & 10:

- RAI in Legal domain
- RAI in Health care domain
- RAI in Education domain
- A few other domains
- Policy issues in RAI

Week 11 & 12:

- Couple of panel discussion with industry practitioners, academic, government (possibly), and others.
- Fireside chat with eminent personalities
- Recorded Paper reading discussion

Ethical Hacking

Duration :	12 weeks
Category :	Computer Science and Engineering

Course layout

Week 1: Introduction to ethical hacking. Fundamentals of computer networking. TCP/IP protocol stack.

Week 2: IP addressing and routing. TCP and UDP. IP subnets.

Week 3: Routing protocols. IP version 6.

Week-4: Installation of attacker and victim system. Information gathering using advanced google search, archive.org, netcraft, whois, host, dig, dnsenum and NMAP tool.

Week-5: Vulnerability scanning using NMAP and Nessus. Creating a secure hacking environment. System Hacking: password cracking, privilege escalation, application execution. Malware and Virus. ARP spoofing and MAC attack.

Week 6: Introduction to cryptography, private-key encryption, public-key encryption.

Week 7: Cryptographic hash functions, digital signature and certificate, applications.

Week 8: Steganography, biometric authentication, network-based attacks, DNS and Email security.

Week-9: Packet sniffing using wireshark and burpsuite, password attack using burp suite. Social engineering attacks and Denial of service attacks.

Week 10: Elements of hardware security: side-channel attacks, physical inclinable functions, hardware trojans.

Week-11: Different types of attacks using Metasploit framework: password cracking, privilege escalation, remote code execution, etc. Attack on web servers: password attack, SQL injection, cross site scripting.

Week 12: Case studies: various attacks scenarios and their remedies.

Introduction to Large Language Models (LLMs)

Weeks: 12 weeks

Course layout

Week 1

1. Course Introduction
2. Introduction to NLP (NLP Pipeline, Applications of NLP)

Week 2

1. Introduction to Statistical Language Models
2. Statistical Language Models: Advanced Smoothing and Evaluation

Week 3

1. Introduction to Deep Learning (Perceptron, ANN, Backpropagation, CNN)
2. Introduction to PyTorch

Week 4

1. Word Representation
 - a. Word2Vec, fastText
 - b. GloVe
2. Tokenization Strategies

Week 5

1. Neural Language Models
 - a. CNN, RNN
 - b. LSTM, GRU
2. Sequence-to-Sequence Models, Greedy Decoding, Beam search
3. Other Decoding Strategies: Nucleus Sampling, Temperature Sampling, Top-k Sampling
4. Attention in Sequence-to-Sequence Models

Week 6

1. Introduction to Transformers
 - a. Self and Multi-Head Attention
 - b. Positional Encoding and Layer Normalization
2. Implementation of Transformers using PyTorch

Week 7

1. Pre-Training Strategies: ELMo, BERT (Encoder-only Model)
2. Pre-Training Strategies: Encoder-decoder and Decoder-only Models
3. Introduction to HuggingFace

Week 8

1. Instruction Tuning
2. Prompt-based Learning
3. Advanced Prompting Techniques and Prompt Sensitivity
4. Alignment of Language Models with Human Feedback (RLHF)

Week 9

1. Open-book question answering: The case for retrieving from structured and unstructured sources; retrieval-augmented inference and generation
2. Retrieval augmentation techniques
 - a. Key-value memory networks in QA for simple paths in KGs
 - b. Early HotPotQA solvers, pointer networks, reading comprehension
 - c. REALM, RAG, FiD, Unlimiformer
 - d. KGQA (e.g., EmbedKGQA, GrailQA)

Week 10

1. Knowledge graphs (KGs)
 - a. Representation, completion
 - b. Tasks: Alignment and isomorphism
 - c. Distinction between graph neural networks and neural KG inference

Week 11

1. Parameter-efficient Adaptation (Prompt Tuning, Prefix Tuning, LoRA)
2. An Alternate Formulation of Transformers: Residual Stream Perspective
3. Interpretability Techniques

Week 12

1. Overview of recently popular models such as GPT-4, Llama-3, Claude-3, Mistral, and Gemini
2. Ethical NLP – Bias and Toxicity
3. Conclusion

AI in Human Resource Management

Duration :	12 weeks
Category :	<ul style="list-style-type: none">○ Management Studies○ Human Resource Management

Course layout

Week 1: Understanding AI

Lecture 1: Deploying AI in HR Practices

Lecture 2: Introduction to AI tools

Lecture 3: Leveraging AI for Diversity Management

Week 2: Adopting AI in HR practices

Lecture 1: Decision making

Lecture 2: Adoption of AI in Task automation, Recruitment, and Talent acquisition

Lecture 3: HR Metrics

Week 3: AI in Performance Management, Onboarding, Person-job fit (Part-1)

Lecture 1: Role of AI in Performance Management

Lecture 2: Application of AI in Onboarding

Lecture 3: Using AI in Person -job fit

Week 4: AI in HR analytics, People analytics, SMART HRM (Part-2)

Lecture 1: HR Analytics

Lecture 2: People Analytics Using AI

Lecture 3: HR administration application

Lecture 4: SMART HRM

Week 5: Usage of AI in various functions of HR

Lecture 1: Using AI for Employee Retention

Lecture 2: Using AI in Performance Appraisal

Lecture 3: Using AI in Employee Training

Lecture 4: Using AI in Workforce Planning

Lecture 5: Ethical concerns in using AI in various functions of HRM

Week 6: Innovation & HR(Part-1)

Lecture 1: AI-Augmented HRM

Lecture 2: Learning and Development Programmes

Lecture 3: Disruptive innovation in HRM: Future of HRM

Week 7: Innovation & HR (Part-2)

Lecture 1: HRM in the era of Generative AI

Lecture 2: Building Organizational Capabilities through AI Driven HRM

Lecture 3: Metaverse in HRM

Week 8: Challenges and Future Opportunities of AI in HRM

Lecture 1: Challenges of AI adoption in HRM

Lecture 2: HRM digitalization Success and Future Opportunities.

Lecture 3: AI in Career Succession Planning of Employees

Week 9: Emerging Trends of AI in HRM (Part-1)

Lecture 1: AI in Sustaining Green HRM

Lecture 2: Emerging trends of AI based HRM

Lecture 3: Benefits of Synergizing AI and HRM

Week 10: Emerging Trends of AI in HRM (Part-2)

Lecture 1: AI in Compensation & Benefits

Lecture 2: AI in Compliance

Lecture 3: AI- Mediated Knowledge Management

Week 11: AI tools and Employee Experiences

Lecture 1: AI in SHRM

Lecture 2: HRP& HR Chatbots

Lecture 3: Using AI in enhancing employee experience

Week 12: AI and Company Culture and its concomitance with HR Practices

Lecture 1: HR & Company Culture

Lecture 2: Adopting AI in Managing Company Culture

Lecture 3: Boon or Curse: Co-existence of HR & AI

Artificial Intelligence in Drug Discovery and Development

Duration :	12 weeks
Category :	<ul style="list-style-type: none">○ Chemical Engineering○ Computational Biology

Course layout

Week 1: Basics of drug discovery pipeline

1. Drug discovery and development
2. Overview of drug discovery workflows
3. Drug design strategies
4. Conventional methods for drug discovery
5. Riddles in drug discovery

Week 2: Introduction to AI in drug discovery and development

1. History and evolution of AI in drug discovery
2. Overview of AI technologies
3. Key applications of AI across the pipeline
4. Available AI tools and platforms
5. Advantages of AI integration in drug discovery

Week 3: Fundamentals of AI and ML techniques

1. Introduction to machine learning concepts
2. Overview of neural networks
3. Feature engineering and data preprocessing
4. Evaluation metrics for AI models
5. Introduction to Python libraries for AI in drug discovery

Week 4: AI in target identification, prediction and validation

1. Introduction to biological targets
2. Basics of target identification and validation
3. Omics data integration for target discovery
4. Binding site and protein structure prediction with AI
5. Hands-on tutorial: Protein structure prediction

Week 5: AI in high throughput virtual screening and lead identification

1. Introduction and approaches to virtual screening
2. AI tools for virtual screening
3. AI assisted molecular docking

4. Workflow of high-throughput virtual screening
5. Hands-on tutorial: AI-assisted molecular docking

Week 6: AI in lead optimization and drug-target interaction

1. Basics of lead optimization
2. AI for drug-target interaction studies
3. QSAR modelling
4. Molecular dynamics simulations
5. Hands-on tutorial: Molecular dynamics trajectory analysis

Week 7: ADMET predictive modelling in drug discovery

1. Introduction to ADMET Properties
2. Importance in lead optimization
3. Conventional methods for ADMET prediction
4. Open available resources for ADMET prediction
5. Hands-on tutorial: AI-enabled ADMET prediction

Week 8: AI in clinical phase

1. Overview of clinical trials
2. Patient recruitment, stratification, and retention
3. Clinical trial protocol design and optimization
4. Predicting outcomes of clinical trials with AI
5. Data collection and monitoring for regulatory submissions

Week 9: De Novo Drug Design using Generative AI

1. Introduction to Generative AI in drug design
2. Deep Generative Models for drug design (GAN, GNN, RNN, VAE etc.)
3. Benchmarking Generative Models for drug design
4. Molecule optimization with Generative AI
5. Hands-on tutorial: AI-powered de novo drug design

Week 10: Advanced concepts: Precision medicine, Network pharmacology and Drug repurposing

1. AI in genomics for personalized treatments
2. AI in real-time monitoring and feedback
3. Overview and data sources for AI in drug repurposing
4. Integrating multi-target drug discovery
5. Network pharmacology with AI

Week 11: Case studies, challenges, future directions, and resources

1. Public AI resources for drug discovery
2. Examples of notable successful case studies
3. Challenges in modern drug discovery realm
4. Regulatory considerations for AI implementation in drug development
5. Future outlook: Explainable artificial intelligence, (XAI) and other emerging technologies in drug discovery

Week 12: Hands-on sessions (Implementing an advanced workflow for molecular structure representation, property prediction, and ultra-large virtual screening)

1. Molecular structure representation
2. ML-assisted solubility prediction

3. AI-assisted bioactivity prediction
4. Pharmacophore- based ultra-large virtual screening
5. Similarity based virtual screening

AI in Product Management

Duration :	12 weeks
Category :	Management Studies

Course layout

Week 1: Introduction to Product Management, Role of AI in Product Management (Part-I, II, III), AI-Powered Market Research

Week 2: AI-Powered Market Research Tools, Analyzing Qualitative Data with AI, Enhancing Quantitative Research with AI, AI in Customer Sentiment Analysis, Predictive Analytics in Market Research

Week 3: AI in Brainstorming & Idea Generation, Validating Ideas using AI, AI-Driven Prioritization, Integrating AI into Marketing Planning, Market and Category Analysis with AI

Week 4: AI Tools for Customer Segmentation, Personalization Engines using AI, AI in Omni-Channel Customer Engagement, AI Driven Customer Journey Mapping, Introduction to Competitor Analysis using AI

Week 5: Competitive Intelligence with AI, Competitor Monitoring using AI, Using AI to Predict Competitor Moves, Case Studies on AI in Competitor Analysis, Sales Forecasting Models using AI

Week 6: AI Tools for Demand Planning, AI for Sales Strategy Development, AI in Sales Training, Risk Modeling and Scenario Analysis with AI, Strategic Planning with AI Insights

Week 7: Positioning and Differentiation using AI, AI in Brand Management, Product Lifecycle Management with AI, Case Studies on AI in Product Strategy, Product-Led Growth using AI

Week 8: New Product Development using AI (Part I, II), Transforming New Product Development: The impact of AI (Part I, II), AI in Go-To-Market Strategies

Week 9: Price Optimization using AI (Part I, II, III, IV, V)

Week 10: Agile Development using AI, Roadmap Development using AI, AI for Minimum Viable Product (Part I, II), AI-Powered Advertising (Part I)

Week 11: AI-Powered Advertising (Part II), AI in Channel Management, Distribution Optimization using AI (Part I, II), AI in Performance Monitoring

Week 12: Revenue and profitability Analysis using AI, Benchmarking and Adjustments using AI, Customer support using AI, Challenges & Ethical Considerations, Future Trends in AI for Product Management

AI for Investments

Duration :	12 weeks
Category :	Management Studies

Course layout

Week 1: Introduction to financial markets: Risk-Return Analysis in Investment Decisions – Measures of Risk and Return, understanding value of a firm, goals of a firm, cash flow discounting, making investment decisions, valuation of fixed income securities and common stocks, introduction to portfolio theory and asset pricing models, cost of capital.

Week 2: Overview of AI and machine learning models: Probability modelling, inferential statistics, Supervised and Unsupervised learning algorithms, regression and classification algorithms.

Week 3: Introduction to R Programming, R Fundamentals, Exploratory data analysis and data visualization with R. Statistical Analysis with R, Inferential statistics and hypothesis testing with R.

Week 4: Market Microstructure and Liquidity: Order-driven vs. Quote-driven markets, Market efficiency, Risk preferences, Limit order books, market microstructure types, economic theory of choice, interest rate compounding

Week 5: Portfolio construction: Portfolio risk and expected returns for two securities and multiple securities, risk diversification with portfolios, correlation structure, mean-variance framework, portfolio construction with R

Week 6: Portfolio Optimization: Portfolio Possibility curve, Efficient frontier, Minimum Variance portfolios, Introduction to risk-free lending and borrowing, market risk and beta, portfolio optimization with R

Week 7: Asset Pricing Models: Capital Asset Pricing Model (CAPM), Capital Market Line, Security Market Line, Fallings of CAPM, Single-Index and Multi-Index models, Expected Risk and Return with Index models, 3-Factor Fama-French Model

Week 8: Portfolio Management and Performance Evaluation: Portfolio Management strategies, Active vs Passive Portfolio Management, Value vs Growth investing, One-parameter performance measures Timing & Selection performance measures, application of asset pricing models in performance management

Week 9: Introduction to Algorithmic Trading: Technical analysis and trend determination, Dow Theory, Moving averages, Momentum indicators, Classical price patterns.

Week 10: AI and machine learning in Trading execution and portfolio management: Regression and Classification algorithm applications in security analysis, forecasting, and prediction, Case Study examples

Week 11: Advanced time-series regression algorithms: Panel regression quantile regression, ARMA/ARIMA models, Mean reverting trading strategies with vector error correction models and cointegration, model risk management, back testing, model validation, and stress testing with R

Week 12: Advanced time-series algorithms for financial risk-management: Value-at-risk, Expected Shortfall, ARCH/GARCH models, implementation with R

Food Science and Technology

Duration :	12 weeks
Category :	Agricultural and Food Engineering Food Process Engineering

Course layout

Week 1: Food, Sustainability and Health: Nature and types of foods; Food production and processing challenges; Global warming and management of food losses; Energy and nutritional value of foods, Balance diets - access and affordability; Consumer awareness and behaviour; Technology & resource barriers.

Week 2: Food Structure-Function Relationship: Food quality characteristic, chemical composition and physical structure; Physical, textural and rheological characteristics of food; Thermal properties relationship; Relationship of structure to quality.

Week 3: Major Chemical Processes in Food : Major chemical and biochemical reactions during food processing, handling and storage; Chemical interactions among major food constituents – carbohydrates, protein, lipids; Hydrolysis & oxidation (enzymatic & non-enzymatic) reactions; Factors affecting changes during processing and storage; Enzyme catalysed reactions.

Week 4: Sensory Quality Attributes of Food : Significance of sensory organs; Anatomy and functions of taste and smell; Sensory evaluation (subjective and objective) methods; Psychophysics of sensory perception; Novel techniques in sensory evaluation- e-Tongue, e-Nose, etc; Consumer acceptability.

Week 5: Food Macronutrients – Structure and Function: Structure of water and ice, free and bound water, water activity (aw) and food stability; Types, structure and function of carbohydrates, lipids and proteins; Browning reactions, rancidity and protein denaturation.

Week 6: Micronutrients and Bioactive Compounds in Food: Sources, structure and functions of vitamins and minerals; Importance of micronutrients in human nutrition and health, stability of micronutrients during processing and storage; Phytochemicals and bioactive compounds; Pigments and colours; Flavouring compounds.

Week 7: Microorganism Associated with Foods: Introduction to food microorganisms – bacteria, yeast and moulds; Microbial growth - kinetic model, factors influencing growth of microorganisms in foods; Microbial death kinetics and factors affecting; Probiotics and

bacteriocins, Microbial spoilage of foods; Food poisoning.

Week 8: Food Additives and Contaminants: Definition, types and roles of chemical additives in foods; Functional food additive applications; Food adulteration – types, detrimental effects and detection; Natural food toxins, allergens, anti-nutrients and contaminants. International regulations on food additives.

Week 9: Food Preservation Principles: Traditional and modern methods of food preservation; Preservation of foods by addition of chemicals and removal of water; Biopreservation of foods; Low-temperature and non-thermal preservation; Alternative/advanced thermal techniques; Combined preservation technologies; Food packaging.

Week 10: Food Formulation and Processing: Food process operations and principles; Ingredient preparation, formulation and metering; Mathematical tools for food formulation; New food product development; Batch and continuous processing; Functional and designer foods; 3D printed foods for personalized nutrition

Week 11: Food Manufacturing and Industry 4.0: Concepts in food manufacturing; Good manufacturing practices and Food industry 4.0; Internet of things (IoT) for real time data collection and analysing; AI-ML applications in food industry; Predictive maintenance; Process control instrumentation and sensors; Automation and Robotics.

Week 12: Circular Economy in Food Industry: Concept of circular economy – reducing wastes, reusing & recycling, sustainable sourcing and resource efficiency; Food industry byproduct processing, waste utilization and valorisation; Green processing and packaging.

Machine Learning for Soil and Crop Management

Duration :	12 weeks
Category :	Agricultural and Food Engineering

Course layout

Week 1: General Overview Of ML And DL Applications In Agriculture

Week 2: Basics Of Multivariate Data Analytics

Week 3: Principal Component Analysis And Regression Applications In Agriculture

Week 4: Applications Of Classification And Clustering Methods In Agriculture

Week 5: Diffuse Reflectance Spectroscopy: Basics And Applications For Crop And Soil

Week 6: Use Of ML For Portable Proximal Soil And Crop Sensors

Week 7: ML And DL For Soil And Crop Image Processing

Week 8: UAV And ML Applications In Agriculture

Week 9: Hyperspectral Remote Sensing And ML Applications In Agriculture

Week 10: Digital Soil Mapping – General Overview

Week 11: Digital Soil Mapping With Continuous Variables

Week 12: Digital Soil Mapping With Categorical Variables

Carbon Accounting and Sustainable Designs in Product Lifecycle Management

Course layout

Week 1: Productivity and Sustainability

- Productivity and Sustainability
- Measuring Productivity
- Measures Affecting Productivity
- Productivity and Sustainability (Part-2)
- Environmental Management System

Week 2: Introduction to Carbon Footprint Systems

- Green System
- Carbon Footprint
- Carbon Credit Trading
- Industrial Ecology and Carbon Footprint
- Examples of Carbon Footprint Calculations

Week 3: Carbon Footprint and Green Manufacturing

- Examples of Carbon Footprint Calculations (Part-2)
- Some More Green Thoughts and Footprints
- Green Manufacturing
- Partnership for a New Generation of Vehicles (PNGV)

Week 4: Road to Product Lifecycle Management

- Smart Design and Engineering
- Road to Product Lifecycle Management (Part-1)
- Road to Product Lifecycle Management (Part-2)
- Road to Product Lifecycle Management (Part-3)

Week 5: Sustainability and Green Supply Chain

- Sustainability and Green Supply Chain (Part-1)
- Sustainability and Green Supply Chain (Part-2)
- Energy Transformations
- PLM Components and levels (Part-1)
- PLM Components and levels (Part-2)

Week 6: PLM Integration with the Carbon Accounting

- PLM integration (Part-1)
- PLM integration (Part-2)
- Facility Carbon Accounting
- Activities of emission (Part-1)
- Activities of emission (Part-2)

Week 7: Carbon Accounting and Business Data

- Carbon and business data (Part-1)
- Carbon and business data (Part-2)
- Carbon and business data (Part-3)
- Carbon Accounting Model (Part-1)
- Carbon Accounting Model (Part-2)

Week 8: Modeling for Carbon Accounting

- Carbon Accounting Model (Part-1)
- Carbon Accounting Model (Part-2)
- Carbon Accounting Model (Part-3)
- Carbon Accounting Model (Part-4)
- Carbon Accounting Model (Part-5)

Week 9: PLM Systems, ESG, and Carbon Accounting Databases

- Integrated PLM, SLM and ALM
- Environmental, Social, and Governance (ESG) Systems
- Carbon Accounting Databases (Part-1)
- Carbon Accounting Databases (Part-2)
- Carbon Accounting Databases (Part-3)

Week 10: DBMS: Design and Terminologies

- Database Management Systems
- Database Design
- Terminologies in Database Design (Part-1)
- Terminologies in Database Design (Part-2)

Week 11: Database Schema and Normalization for Carbon Accounting

- Database Schema (Part-1)
- Database Schema (Part-2)
- Database Normalization (Part-1)
- Database Normalization (Part-2)

Week 12: Carbon Accounting User Interface

- Carbon Accounting User Interface (Part-1)
- Carbon Accounting User Interface (Part-2)
- Carbon Accounting User Interface (Part-3)

Entrepreneurship

Course layout

The course structure and content covers, over a period of 12 weeks, the following 15 modules.

Module 1: Entrepreneurial Journey

Module 2: Entrepreneurial Discovery

Module 3: Ideation and Prototyping

Module 4: Testing, Validation and Commercialisation

Module 5: Disruption as a Success Driver

Module 6: Technological Innovation and Entrepreneurship – 1

Module 7: Technological Innovation and Entrepreneurship – 2

Module 8: Raising Financial Resources

Module 9: Education and Entrepreneurship

Module 10: Beyond Founders and Founder-Families

Module 11: India as a Start-up Nation

Module 12: National Entrepreneurial Culture

Module 13: Entrepreneurial Thermodynamics

Module 14: Entrepreneurship and Employment

Module 15: Start-up Case Studies

Six Sigma

Course layout

Week 1 : QUALITY: FUNDAMENTALS AND KEY CONCEPTS

- Lecture 1: Brief overview of the course
- Lecture 2: Quality concepts and definition
- Lecture 3: History of continuous improvement
- Lecture 4: Six Sigma Principles and Focus Areas (Part 1)
- Lecture 5: Six Sigma Principles and Focus Areas (Part 2)
- Lecture 6: Six Sigma Applications

Week 2 : QUALITY: FUNDAMENTALS AND KEY CONCEPTS

- Lecture 7: Quality Management: Basics and Key Concepts
- Lecture 8: Fundamentals of Total Quality Management
- Lecture 9: Cost of quality
- Lecture 10: Voice of customer
- Lecture 11: Quality Function Deployment (QFD)
- Lecture 12: Management and Planning Tools (Part 1)
- Lecture 13: Management and Planning Tools (Part 2)

Week 3 : DEFINE

- Lecture 14: Six Sigma Project Identification, Selection and Definition
- Lecture 15: Project Charter and Monitoring
- Lecture 16: Process characteristics and analysis
- Lecture 17: Process Mapping: SIPOC

Week 4 : MEASURE

- Lecture 18: Data Collection and Summarization (Part 1)
- Lecture 19: Data Collection and Summarization (Part 2)
- Lecture 20: Measurement systems: Fundamentals
- Lecture 21: Measurement systems analysis: Gage R&R study
- Lecture 22: Fundamentals of statistics
- Lecture 23: Probability theory

Week 5 : MEASURE

- Lecture 24: Process capability analysis: Key Concepts
- Lecture 25: Process capability analysis: Measures and Indices
- Lecture 26: Process capability analysis: Minitab Application
- Lecture 27: Non-normal process capability analysis

Week 6 : ANALYZE

- Lecture 28: Hypothesis testing: Fundamentals
- Lecture 29: Hypothesis Testing: Single Population Test
- Lecture 30: Hypothesis Testing: Two Population Test
- Lecture 31: Hypothesis Testing: Two Population: Minitab Application
- Lecture 32: Correlation and Regression Analysis
- Lecture 33: Regression Analysis: Model Validation

Week 7 : ANALYZE

- Lecture 34: One-Way ANOVA

Lecture 35: Two-Way ANOVA

Lecture 36: Multi-vari Analysis

Lecture 37: Failure Mode Effect Analysis (FMEA)

Week 8 : IMPROVE

Lecture 38: Introduction to Design of Experiment

Lecture 39: Randomized Block Design

Lecture 40: Randomized Block Design: Minitab Application

Lecture 41: Factorial Design

Lecture 42: Factorial Design: Minitab Application

Week 9 : IMPROVE

Lecture 43: Fractional Factorial Design

Lecture 44: Fractional Factorial Design: Minitab Application

Lecture 45: Taguchi Method: Key Concepts

Lecture 46: Taguchi Method: Illustrative Application

Week 10 : CONTROL

Lecture 47: Seven QC Tools

Lecture 48: Statistical Process Control: Key Concepts

Lecture 49: Statistical Process Control: Control Charts for Variables

Lecture 50: Operating Characteristic (OC) Curve for Variable Control charts

Lecture 51: Statistical Process Control: Control Charts for Attributes

Lecture 52: Operating Characteristic (OC) Curve for Attribute Control charts

Lecture 53: Statistical Process Control: Minitab Application

Week 11 : CONTROL

Lecture 54: Acceptance Sampling: Key Concepts

Lecture 55: Design of Acceptance Sampling Plans for Attributes (Part 1)

Lecture 56: Design of Acceptance Sampling Plans for Attributes (Part 2)

Lecture 57: Design of Acceptance Sampling Plans for Variables

Lecture 58: Acceptance Sampling: Minitab Application

Week 12 : SIX SIGMA IMPLEMENTATION CHALLENGES

Lecture 59: Design for Six Sigma (DFSS): DMADV, DMADOV

Lecture 60: Design for Six Sigma (DFSS): DFX

Lecture 61: Team Management

Lecture 62: Six Sigma: Case study

Lecture 63: Six Sigma: Summary of key concepts

Sustainable energy technology

Week1: Introduction and Fundamental Concepts - Part 1 | Sustainable Energy Technology

Week2: Impact of Fossil fuels - Part 1| Sustainable Energy Technology

Week3: Renewable Energy Contributions - Part 1| Sustainable Energy Technology

Week4: Introduction to Wind Energy - Part 1| Sustainable Energy Technology

Week5: Introduction to Wind Energy - Part 1| Sustainable Energy Technology

Week6: Introduction to Solar Photovoltaic Systems - Part 1| Sustainable Energy Technology

Week7: Types of solar cells - Part 1| Sustainable Energy Technology

Week8: Introduction of Geothermal Energy | Sustainable Energy Technology

Week9: Mechanical Energy Storage Technologies | Sustainable Energy Technology

Week10: Electrochemical Energy Storage Systems | Sustainable Energy Technology

Week11: Storage of Coolness and Synoptic View of Energy Storage Technology | Sustainable Energy Technology

Week12: Hydrogen production and storage technologies | Sustainable Energy Technology