|  |  |
| --- | --- |
| D:\Shiv@SIT\IMPORTANT docs SIT\LOGOs\LOGO HD.png | **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) (w.e.f. 2025-26)**

**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 |
|  | IPCC |  | Artificial Neural Network and Deep Learning (I) |  | | 42 | 0 | | 28 |  | 3 | 50 | 50 | 100 | 4 |
|  | IPCC |  | Generative AI and Prompt Engineering(I) |  | | 42 | 2 | | 0 |  | 3 | 50 | 50 | 100 | 4 |
|  | PCC |  | Federated Learning |  | | 42 | 0 | | 28 |  | 3 | 50 | 50 | 100 | 4 |
|  | PEC |  | Professional Elective Course-III |  | | 42 | 0 | | 0 |  | 3 | 50 | 50 | 100 | 3 |
|  | OEC |  | Open Elective Course-II |  | | 42 | 0 | | 0 |  | 3 | 50 | 50 | 100 | 3 |
|  | PROJ |  | 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)** | | | | | | | | | | | | | | | |
|  | | Explainable and Responsible AI | | |  | | | AI in Data Security & Privacy | | | | | | | |
|  | | Robotic Process Automation | | |  | | | Blockchain traced AI | | | | | | | |
|  | | 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. | | | | | | | | | | | | | | | |

|  |  |
| --- | --- |
| D:\Shiv@SIT\IMPORTANT docs SIT\LOGOs\LOGO HD.png | **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 Artificial Intelligence & Data Science** |

|  |
| --- |
| **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. |

|  |  |  |  |
| --- | --- | --- | --- |
| B.E. COMPUTER SCIENCE & ENGINEERING  **(ARTIFICIALINTELLIGENCE AND MACHINE LEARNING)**  Outcome Based Education (OBE) and Choice Based Credit System (CBCS)  **SEMESTER - VII** | | | |
| **ARTIFICIAL NEURAL NETWORK AND DEEP LEARNING (I)** | | | |
| Course Code |  | 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: | |
|  | Get introduced the fundamental concepts of neural networks, including neuron models, network architectures, and biological inspiration |
|  | Analyze and implement single-layer and multilayer perceptron models, with a focus on learning algorithms like back propagation. |
|  | Explore techniques for improving neural network training through regularization, data augmentation, and optimization strategies. |
|  | Understand the structure and functioning of Convolutional Neural Networks (CNNs) and their role in processing spatial data. |
|  | 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 | |
|  | **Describe** the structure and function of artificial neural networks and relate them to biological neural systems. |
|  | **Implement** perceptron and multilayer perceptron models using learning algorithms such as back propagation. |
|  | **Apply** regularization and optimization techniques to enhance the performance and generalization of deep learning models. |
|  | **Design and evaluate** Convolutional Neural Networks (CNNs) for applications involving image and spatial data processing. |
|  | **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** |  |  |  |  |  |  |  | **2** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **B.E. COMPUTER SCIENCE & ENGINEERING**  **(ARTIFICIALINTELLIGENCE AND MACHINE LEARNING)**  Outcome Based Education (OBE) and Choice Based Credit System (CBCS)  **SEMESTER - VII** | | | |
| **GENERATIVE AI AND PROMPT ENGINEERING(I)** | | | |
| Course Code |  | 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 | 1st 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 | 1st 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**  **(ARTIFICIALINTELLIGENCE AND MACHINE LEARNING)**  Outcome Based Education (OBE) and Choice Based Credit System (CBCS)  **SEMESTER - VII** | | | |
| **FEDERATED LEARNING** | | | |
| Contact Hours/ Week: |  | Credits: | 50 |
| Total Lecture Hours: | (3:0:0) | CIE Marks: | 50 |
| Course Code: | 3 | SEE Marks: | 3 |
|  | 42Hrs |  | 28hrs |

|  |  |
| --- | --- |
| **Course objectives:**  This course will enable students to: | |
|  | Understand the foundational concepts of Federated Learning (FL). |
|  | Explore the different FL architectures and algorithms. |
|  | Learn privacy-preserving techniques and their implementation in FL |
|  | Apply FL methods to real-world scenarios |
|  | 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 AveragingAlgorithm,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 ProfitSharing 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 forRecommendation 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. | *IEEE Transactions on Neural Networksand Learning Systems*. | 2022 |
| 3 | A survey on federated learning systems: Vision, hype andreality for data privacy and protection | Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., Li, Y | *IEEE Transactions on Knowledge and Data Engineering*, | 2021 |

|  |  |
| --- | --- |
| **Course Outcomes:** Upon completion of this course the student will be able to: | |
| 1 | Understand the foundational principles and design of Federated Learning. |
| 2 | Implement and utilize various FL algorithms and architectures. |
| 3 | Address privacy and security issues in Federated Learning systems. |
| 4 | Apply Federated Learning techniques to real-world scenarios and evaluate their performance. |
| 5 | Understand the significance of Federated Learning for Vision, Language, and Recommendation |

**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** |  |  |
| **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 |  | 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](https://www.amazon.com.au/Responsible-AI-Practices-Creating-Trustworthy/dp/0138073929) AI systems | **Qinghua Lu, Liming Zhu, Jon Whittle, Xiwei Xu** | Addison-Wesley Professional | Edition 1, 26 December 2023 |
| 2 | Explainable AI for Practitioners | [Michael Munn](https://dokumen.pub/explainable-ai-for-practitioners-early-release-ch1amp2-8-9781098119133.html#Michael+Munn), [David Pitman](https://dokumen.pub/explainable-ai-for-practitioners-early-release-ch1amp2-8-9781098119133.html#David+Pitman) | O'Reilly Media, Inc. | Edition1, October 2022 |
| **Reference Books** | | | | |
| 1 | Towards ethical and socially responsible explainable AI : challenges and oppurtunities | [Mohammad Amir, Khusru Akhtar](https://link.springer.com/book/10.1007/978-3-031-66489-2#author-0-0) , [Mohit Kumar](https://link.springer.com/book/10.1007/978-3-031-66489-2" \l "author-0-1) ,  [Anand Nayyar](https://link.springer.com/book/10.1007/978-3-031-66489-2#author-0-2) | Springer cham | Edition 1, August 2024 |
| 2 | Explainable and Responsible Artificial Intelligence in Healthcare | [Rishabha, Malviya,](https://www.wiley.com/en-us/search?filters%5bauthor%5d=Rishabha%20Malviya&pq=++) Sonali , Sundram | Wiley, | Edition 1, March 2025 |
| 3 | Responsible AI in practice: A practical guide to safe and human AI | [Toju Duke](https://link.springer.com/book/10.1007/979-8-8688-1166-1#author-0-0) , [Paolo Giudici](https://link.springer.com/book/10.1007/979-8-8688-1166-1#author-0-1) | 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 |  | 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-APls- Al-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 PIay - Downloading and installing UiPath Studio -Learning Ui Path Studio- - Task recorder - Step-by-step, Examples using the recorder.  **Textbook 2= Ch l, 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,lSBN-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 toRobotic 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](https://www.amazon.in/s/ref=dp_byline_sr_ebooks_1?ie=UTF8&field-author=Richard+Murdoch&text=Richard+Murdoch&sort=relevancerank&search-alias=digital-text) | 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](https://www.amazon.in/Srikanth-Merianda/e/B01M5INNL5/ref=dp_byline_cont_book_1) | 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**  **(ARTIFICIALINTELLIGENCE AND MACHINE LEARNING)**  Outcome Based Education (OBE) and Choice Based Credit System (CBCS)  **SEMESTER - VII** | | | |
| **AI IN DATA SECURITY & PRIVACY** | | | |
| Course Code |  | 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** |
| **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  **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. |

|  |
| --- |
| **UNIT V 8 Hours** |
| **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. |

|  |  |
| --- | --- |
| **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 | [Anyu Wang](https://www.worldscientific.com/author/Wang%2C+Anyu) (*Cloud Security Alliance Great China Region, China*) | World Scientific | April 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 | 1 |  |  |  |  |  |  |  |  |  |  | 2 |  |
| **CO2** | 2 |  | 2 |  |  |  |  |  |  |  |  |  | 2 |  |
| **CO3** | 2 | 2 |  |  |  |  |  |  |  |  |  |  | 2 |  |
| **CO4** | 2 | 1 |  |  |  |  |  |  |  |  |  |  | 2 |  |
| **CO5** | 2 |  | 2 |  |  |  |  |  |  |  |  |  | 2 |  |
| **Overall CO** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**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** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **B.E. COMPUTER SCIENCE & ENGINEERING**  **(ARTIFICIALINTELLIGENCE AND MACHINE LEARNING)**  Outcome Based Education (OBE) and Choice Based Credit System (CBCS)  **SEMESTER - VII** | | | |
| **BLOCKCHAIN TRACED AI** | | | |
| Course Code |  | 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 | |
|  | Describe the concepts of Blockchain and its structure. |
|  | Outline the prerequisite concepts of Blockchain. |
|  | Illustrate the working of Bitcoin cryptocurrency. |
|  | Demonstrate the concepts of Blockchain on Ethereum platform for a suitable application. |
|  | 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** |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **B.E. COMPUTER SCIENCE & ENGINEERING**  Outcome Based Education (OBE) and Choice Based Credit System (CBCS)  **SEMESTER - VII** | | | |
| **AGENTIC AI – FOUNDATIONS AND APPLICATIONS** | | | |
| Course Code |  | 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** |  |