SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
21AI701T	Expert Systems in Artificial Intelligence	3	-	-	3	30	70	100

Course Objectives	Course Outcomes
This course is intended to • Learn the basics of an expert system. • Gain knowledge about implementation ofan expert system.	**Students will be able to** • Interpret the basics of the expert system. • Learn theoretical foundation of expert system. • Distinguish the various types of expert systems. • Comprehend the various components of an expert system. • Develop the expert system.

Unit I: Introduction to Expert Systems	**[7Hrs]**
The nature of Expert Systems Types of applications of Expert Systems relationship of Expert Systems to Artificial Intelligence and to Knowledge-Based Systems. The nature of expertise Distinguishing features of Expert Systems. Benefits of using an Expert System Choosing an application.	
Unit II: Inference in Expert Systems	**[7Hrs]**
Theoretical Foundations What an expert system is; how it works and how it is built. Basic forms of inference: abduction; Deduction; induction.	
Unit III: Knowledge base in Expert Systems	**[7Hrs]**
The representation and manipulation of knowledge in a computer; Rule-based representations (with backward and forward reasoning); logic-based representations (with resolution refutation); taxonomies; meronomies; frames (with inheritance and exceptions); semantic and partitioned nets (query handling).	
Unit IV: Development of Expert Systems	**[8Hrs]**
Basic components of an expert system; Generation of explanations; Handling of uncertainties; Truth Maintenance Systems; Expert System Architectures; An analysis of some classic expert systems; Limitations of first generation expert systems; Deep expert systems; Co-operating expert systems and the blackboard model.	
Unit V: Representation and evaluation	**[7Hrs]**
Building Expert Systems Methodologies for building expert systems: knowledge acquisition and elicitation; formalization; representation and evaluation. Knowledge Engineering tools, Case Study.	

Text Books

S.N	Title	Authors	Edition	Publisher
1	Introduction to Expert Systems	P Jackson	2nd	Addison Wesley.
2	Artificial Intelligence	Elaine Rich, Kevin Knight	2nd	McGraw-Hill, Inc.

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Problem Solving and Artificial Intelligence	Jackson. Jean-Louis Lauriere	3rd	Prentice Hall.

SEVEN SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
21AI702P	Software Lab - II	-	-	2	1	CA	ESE	Total
						25	25	50

Course Objectives	Course Outcomes
This course is intended to • Understand and Analyze Transformer-based Architecture • Design and Implement Experiments Using Pre-trained Language Models	**Students will be able to** • Analyze Transformer Architecture • Develop and Evaluate Text Generation with GPT Models: • Implement Sentiment Analysis Using BERT Models • Design and Compare Summarization Techniques • Evaluate linguistic theories through empirical data analysis.

Sr. No.	List of Practicals
1	To study and understand the architecture of Transformer an innovative neural architecture presented by Google researchers in the famous paper Attention is All You Need in 2017– on natural language (NLP) tasks.
2	Develop a code to provide various prompts to GPT-2 and observe how it continues the text. Experiment with different prompt styles (e.g., narrative, dialogue, poetry) and analyze the creativity and coherence of the generated outputs. Compare the results with those generated by GPT-3 or GPT-4 to assess improvements in fluency and creativity over different model versions.
3	Design a program to Input a dataset of sentences into BERT for sentiment analysis. Evaluate its performance by comparing the results with those obtained using RoBERTa or DistilBERT. Discuss the strengths and weaknesses of each model in accurately detecting sentiment in different contexts.
4	Write set of instruction to input lengthy articles into the BART model and generate summaries. Evaluate the generated summaries based on completeness, accuracy, and readability. Compare BART's performance with T5 or other summarization models, discussing the trade-offs between brevity and informativeness.
5	Develop a code to use mBERT to translate text from one language to another. Compare the translations with those produced by OpenAI's GPT or Google's mT5, assessing grammatical correctness, fluency, and fidelity to the original meaning. Discuss the effectiveness of mBERT in handling nuances across languages
6	Provide context paragraphs and questions to ALBERT and evaluate the accuracy and relevance of its answers. Compare the results with those from BERT or XLNet, focusing on the model's ability to understand and respond to complex queries.
7	Write a program to input text samples into RoBERTa for classification tasks, such as spam detection or topic categorization. Compare its classification accuracy and speed with models like BERT or DistilBERT. Discuss scenarios where RoBERTa excels or falls short compared to other models.
8	Use SpaCy's pre-trained NER model to extract entities from a dataset. Validate the results by comparing them with outputs from BERT-NER or Flair, focusing on precision and recall. Discuss the model's ability to generalize across different types of text (e.g., news articles, social media).
Open ended practical	
9	Project on Health Care Dataset
10	Project

Text Books

Sr. No.	Title	Authors	Edition	Publisher
1	Hands-On Large Language Models	Jay Alammar & Maarten Grootendorst	1st	O'Reilly Media
2	Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow, 3rd Edition	Aurelien Geron	1st	O'Reilly Media

Reference Books

Sr. No.	Title	Authors	Edition	Publisher
1	Quick start Guide to Large Language Models	SINAN OZEMIR	1st	Addison-Wesley

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
21AI703T(i)	PE-IV Augmented Reality & Virtual Reality	3	-	-	3	30	70	100

Course Objectives	Course Outcomes
This course is intended to ● Learn the fundamental Computer Vision, Computer Graphics and Human-Computer interaction Techniques related to AR/VR. ● Review the Geometric Modeling Techniques. ● Review the Virtual Environment. ● Discuss and Examine AR/VR Technologies.	**Students will be able to** ● Learn fundamental Computer Vision, Computer Graphics and Human Computer Interaction Techniques related to AR/VR. ● Analyze Geometric Modeling Techniques ● Evaluate the Virtual Environment ● Evaluate AR/VR Technologies. ● Apply various types of Hardware and Software in Virtual Reality systems.

Unit I : Visual Computation In Virtual Reality	**[7Hrs]**
Fundamentals of Computer Graphics-Software and Hardware Technology on Stereoscopic, Display-Advanced Techniques in CG, Management of Large-Scale Environments & Real Time Rendering.	
Unit II: Introduction to Virtual Reality (VR)	**[7Hrs]**
Virtual Reality and Virtual Environment, Computer graphics, Real time computer graphics, Flight Simulation, Virtual environment requirement, benefits of virtual reality, Historical development of VR, Scientific Landmark, Frameworks in Virtual Reality: Frameworks of Software Development Tools in VR. X3D Standard; Vega, MultiGen, Virtools etc.	
Unit III: Introduction Of Augmented Reality	**[7Hrs]**
System Structure of Augmented Reality, Key Technology in AR, AR software development, AR software. Camera parameters and camera calibration, Marker-based augmented reality, Pattern recognition. AR Toolkit.	
Unit IV: Virtual Environment	**[8Hrs]**
Introduction, Virtual environment, Computer environment, VR technology, Model of interaction, VR Systems, Animating the Virtual Environment: Introduction, The dynamics of numbers, Linear and Nonlinear interpolation, the animation of objects, linear and non-linear translation, shape & object in between, free from deformation, particle system	
Unit V: Application of VR in AI And Digital Entertainment	**[7Hrs]**
VR Technology in Film & TV Production. VR Technology in Physical Exercises and Games. Demonstration of Digital Entertainment by VR.3D user interfaces - Why 3D user interfaces. Major user tasks in VE. Interaction techniques for selection, manipulation and navigation.3DUI evaluation. **Application of AI :** Duolingo, Google Earth VR, Labster, Immerse, Dream Box Learning.	

Text Books

S. N	Title	Authors	Edition	Publisher
1	Virtual Reality Technology.	Coiffet, P., Burdea, G. C	1st	Wiley-IEEE Press
2	Augmented Reality: Principles & Practice	Schmalstieg, D., Höllerer, T	1st	Pearson
3.	Wiley Handbook of Human Computer Interaction	Norman, K., Kirakowski, J	1st	Wiley-Blackwell

Reference Books

S. N	Title	Authors	Edition	Publisher
1	Understanding Augmented Reality, Concepts and ApplicationsMachine Learning Engineer	Craig, A. B	1st	Morgan Kaufmann

SEVEN SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
21AI703P(i)	PE-IV Augmented Reality & Virtual RealityLab	-	-	2	1	25	25	50

Course Objectives	Course Outcomes
This course is intended to • Learn the Geometric Modeling Techniques. • Review the Virtual Environment. • Discuss and Examine AR/VR Technologies.	**Students will be able to** • Learn fundamental Computer Vision, Computer Graphics and Human Computer Interaction Techniques related to AR/VR. • Analyze Geometric Modeling Techniques • Evaluate the Virtual Environment • Evaluate AR/VR Technologies. • Apply various types of Hardware and Software in Virtual Reality systems.

Sr. No	List of Practicals
1	Implementation of Computer Graphics.
2	Implementation of Stereoscopic Display
3	Implementation of Real-Time Rendering
4	Implementation of Augmented Reality Development
5	Implementation of Virtual Environment Interaction
6	Implementation of Animation in Virtual Environments
7	Implementation of VR Technology in Digital Entertainment
8	Micro based Project based on studied syllabus.
Open Ended Practical	
9	Implementation of 3D User Interfaces
10	Design and Implement Basic Argument Reality Application

Text Books

Sr. No.	Title	Authors	Edition	Publisher
1	Virtual Reality Technology.	Coiffet, P., Burdea, G. C	1st	Wiley-IEEE Press
2	Augmented Reality: Principles & Practice	Schmalstieg, D., Höllerer, T	1st	Pearson
3.	Wiley Handbook of Human Computer Interaction	Norman, K., Kirakowski, J	1st	Wiley-Blackwell

Reference Books

Sr. No.	Title	Authors	Edition	Publisher
1	Understanding Augmented Reality, Concepts and ApplicationsMachine Learning Engineer	Craig, A. B	1st	Morgan Kaufmann
2	Developing Virtual Reality Applications, Foundations of Effective Design	Craig, A. B., Sherman, W. R., Will,	2nd	Morgan Kaufmann

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
21AI703T(ii)	PE-IV Information Retrieval	3	-	-	3	30	70	100

Course Objectives	Course Outcomes
This course is intended to • Learn the various aspects of an Information retrieval system • Analyze fundamental techniques for hypermedia architectures, design and usability, document management and retrieval, metadata management, and searching the web. • Use advanced techniques for assessing the performance of information retrieval.	**Students will be able to** • Demonstrate the basics of Information Retrieval • Analyze data structures like Inverted Indices used in Information retrieval systems. • Evaluate information retrieval system • Apply different techniques for distributed and multimedia IR • Develop a complete IR system from Scratch

Unit I Introduction to Information Retrieval	**[6Hrs]**
Basic Concepts of IR, Data Retrieval & Information Retrieval, Text mining and IR relation, IR system block diagram, Automatic Text Analysis: Luhn's ideas, Conflation Algorithm, Indexing and Index Term Weighting, Probabilistic Indexing, Automatic Classification. Measures of Association, Different Matching Coefficients, Cluster Hypothesis, Clustering Techniques: Rocchio's Algorithm, Single pass algorithm, Single Link algorithm	
Unit II Indexing and Searching Techniques	**[6Hrs]**
Indexing: Inverted file, Suffix trees & suffix arrays, Signature Files, Scatter storage or hash addressing. Searching Techniques: Boolean Search, sequential search, Serial search, cluster-based retrieval, Query languages, Types of queries, Patterns matching, structural queries. IR Models: Basic concepts, Boolean Model, Vector Model, Probabilistic Model.	
Unit III Evaluation and Visualization of Information Retrieval System	**[6Hrs]**
Performance Evaluation: Precision and recall, MRR, F-Score, NDCG, user-oriented measures. Visualization in Information System: Starting points, Query Specification, document context, User relevance judgment, Interface support for search process.	
Unit IV Distributed and Multimedia IR	**[6Hrs]**
Distributed IR: Introduction, Collection Partitioning, Source Selection, Query Processing. Multimedia IR: Introduction, Data Modelling, Query Language, Background-Spatial Access Method, A Generic Multimedia Indexing Approach, One Dimensional Time Series, Two-Dimensional color Images, Automatic Feature Extraction, Trends and Research Issue	
Unit V Web Searching	**[10Hrs]**
Introduction, Challenges, Web Characteristics, Search Engines: Centralized Architecture, Distributed Architecture, User Interfaces, Ranking, Crawling the web, Indices, Browsing, Meta-searchers, Searching using Hyperlinks, Trends and Research Issues, Introduction to Web Scraping: Python for web scraping, Request, HTML parsing, Beautiful Soup. XML Retrieval: Basic XML concepts, Challenges in XML retrieval, Vector space model for XML retrieval, Evaluation of XML retrieval, Text-Centric vs. Data-Centric XML retrieval. Recommendation System: Collaborative Filtering and Content Based Recommendation of Documents and Products. Introduction to Semantic Web.	

Text Books

Sr. No.	Title	Authors	Edition	Publisher
1	Information Retrieval	Stefan Büttcher, Charles L. A. Clarke	2nd	MIT
2	Modern Information Retrieval: the concepts and technology behind search	Ricardo Baeza- Yates and Berthier Ribeiro – Neto,	3rd	Pearson -
3	Search Engines: Information Retrieval in Practice,	Bruce Croft, Donald Metzler and Trevor Strohman	1st	Pearson,

Reference Books

Sr. No.	Title	Authors	Edition	Publisher
1	Information Storage and Retrieval Systems: Theory and Implementation	Gerald J Kowalski, Mark T Maybury	3rd	Springer
2	Introduction to Information Retrieval	C. Manning, P. Raghavan, and H. Schütze	2nd	Cambridge University Press
3	Information Storage & Retrieval	Dr. Archana K. Ratnaparkh, Jyoti S. Chinchole	1st	NIRALI

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
21AI703P(ii)	Information Retrieval Lab	-	-	2	1	25	25	50

Course Objectives	Course Outcomes
This course is intended to • Learn about building a basic search engine or document retrieval system. • Work on different classification algorithms.	**Students will be able to** • Design IR Model. • Apply Pre-processing in IR Systems. • Design Text based and Web Based Retrieval Systems. • Implement classification algorithms like Naive Bayes, Max Entropy, Rochio's, Support Vector Machine. • Develop a complete IR system from Scratch.

Sr. No.	List of Practical
1	Representation of a Text Document in Vector Space Model and Computing Similarity between two with a total vocabulary size of at least 1000 words.
2	Pre-processing of a Text Document: stop word removal and stemming
3	Construction of an Inverted Index for a given document collection comprising of at least 50 documents with a total vocabulary size of at least 1000 words.
4	Classification of a set of Text Documents into known classes (You may use any of the Classification algorithms like Naive Bayes, Max Entropy, Rochio's, Support Vector Machine). Standard Datasets will have to be used to show the results
5	Text Document Clustering using K-means. Demonstrate with a standard dataset and compute performance measures- Purity, Precision, Recall and F-measure.
6	Crawling/ Searching the Web to collect news stories on a specific topic (based on user input). The program should have an option to limit the crawling to certain selected websites only.
7	Mining Twitter to identify tweets for a specific period (and/or from a geographical location) and identify trends and named entities
8	Implementation of PageRank on Scholarly Citation Network
9	Micro Project
Open Ended Practical	
10	Develop a semantic search engine that leverages natural language processing (NLP) techniques to understand and retrieve relevant information based on user queries.
11	Design and implement a recommender system using collaborative filtering and content-based filtering techniques, and evaluate its performance.

Text Books

Sr. No.	Title	Authors	Edition	Publisher
1	Information Retrieval	Stefan Büttcher, Charles L. A. Clarke	2nd	MIT
2	Modern Information Retrieval: the concepts and technology behind search	Ricardo Baeza- Yates and Berthier Ribeiro – Neto,	3rd	Pearson -
3	Search Engines: Information Retrieval in Practice,	Bruce Croft, Donald Metzler and Trevor Strohman	1st	Pearson,

Reference Books

Sr. No.	Title	Authors	Edition	Publisher
1	Information Storage and Retrieval Systems: Theory and Implementation	Gerald J Kowalski, Mark T Maybury	3rd	Springer
2	Introduction to Information Retrieval	C. Manning, P. Raghavan, and H. Schütze	2nd	Cambridge University Press
3	Information Storage & Retrieval	Dr. Archana K. Ratnaparkh, Jyoti S. Chinchole	1st	NIRALI

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
21AI703T (iii)	PE-IV Computer Vision	3	-	-	3	30	70	100

Course Objectives	Course Outcomes
This course is intended to • Review image processing techniques for computer vision. • Apply various features and recognition techniques of computer vision. • Learn about histogram and binary vision.	**Students will be able to** • Learn low level processing of image and transformation techniques applied to images. • Adapt the feature extraction, segmentation and object recognition methods. • Apply Histogram transform for detection of geometric shapes like line, ellipse and objects. • Illustrate 3D vision process and motion estimation techniques. • Apply vision techniques to real time applications.

Unit I Introduction	**[7Hrs]**
Image Processing, Computer Vision - Low-level, Mid-level, High-level; Fundamentals of Image Formation, Transformation: Orthogonal, Euclidean, Affine, Projective, Fourier Transform, Convolution and Filtering, Image Enhancement, Restoration, Histogram Processing.	
Unit II Feature Extraction and Feature Segmentation	**[7Hrs]**
Feature Extraction -Edges - Canny, LOG, DOG; Line detectors (Hough Transform), Corners - Harris and Hessian Affine, Orientation Histogram, SIFT, SURF, HOG, GLOH, Scale-Space 69 Analysis- Image Pyramids and Gaussian derivative filters, Gabor Filters and DWT. Image Segmentation -Region Growing, Edge Based approaches to segmentation, Graph-Cut, Mean-Shift, MRFs, Texture Segmentation.	
Unit III Images, Histograms, Binary Vision	**[8Hrs]**
Simple pinhole camera model – Sampling – Quantisation – Colour images – Noise – Smoothing – 1D and 3D histograms - Histogram/Image Equalisation - Histogram Comparison - Back-projection - k-means Clustering – Thresholding - Threshold Detection Methods - Variations on Thresholding - Mathematical Morphology – Connectivity.	
Unit IV 3D Vision And Motion	**[7Hrs]**
Methods for 3D vision – projection schemes – shape from shading – photometric stereo – shape from texture – shape from focus – active range finding – surface representations – point-based representation – volumetric representations – 3D object recognition – 3D reconstruction – introduction to motion – triangulation – bundle adjustment – translational alignment – parametric motion–spline-based motion- optical flow – layered motion.	
Unit V Applications	**[7Hrs]**
Overview of Diverse Computer Vision Applications: Document Image Analysis, Biometrics, Object Recognition, Tracking, Medical Image Analysis, Content-Based Image Retrieval, Video Data Processing , Application based on Deep Learning for computer vision.	

Text Books

Sr. No.	Title	Authors	Edition	Publisher
1	Computer Vision: A Modern Approach"	D. A. Forsyth, J. Ponce,	2nd	Pearson Education
2	Computer Vision: Algorithms and Applications	Richard Szeliski	2nd	Springer Verlag London Limited

Reference Books

Sr. No.	Title	Authors	Edition	Publisher
1	Computer Vision: Models, Learning, and Inference	Simon J. D. Prince	2nd	Cambridge University
2	Feature Extraction & Image Processing for Computer Vision,	Mark Nixon and Alberto S. Aquado	3rd	Academic Press
3	Computer & Machine Vision	E. R. Davies	4th	Academic Press

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
21AI703P (iii)	Computer Vision Lab	-	-	2	1	25	25	50

Course Objectives	Course Outcomes
This course is intended to • Learn basic knowledge and theories in image processing and computer vision. • Implement basic and some advanced image processing techniques in OpenCV. • Evaluate Image segmentation, camera calibration and 3D reconstruction.	**Students will be able to** • Implement the basic knowledge, theories and methods in image processing and computer vision. • Adapt basic and some advanced image processing techniques in OpenCV. • Analyze 2D a feature-based based image alignment, segmentation, and motion estimations. • Apply 3D image reconstruction techniques. • Design and develop innovative image processing and computer vision applications.

Sr. No.	List of Practical
1	OpenCV Installation and working with Python
2	Basic Image Processing - loading images, Cropping, Resizing, Thresholding, Contour· analysis, Bolb detection
3	Image Annotation – Drawing lines, text circle, rectangle, ellipse on images
4	Image Enhancement - Understanding Color spaces, color space conversion
5	Histogram equalization, Convolution, Image smoothing, Gradients, Edge Detection
6	Image Features and Image Alignment – Image transforms – Fourier, Hough, Extract· ORB Image features, Feature matching, cloning, Feature matching-based image Alignment
7	Image segmentation using Graphcut / Grabcut
8	Camera Calibration with circular grid, Pose Estimation·
9	Lab based on libraries supported for computer vision such as PyTorch and Fast AI.
10	Micro Project
Open Ended Practical	
11	Object Detection and Tracking using Kalman Filter, Camshift· docs. OpenCV
12	OpenCV/OpenCV-free-course

Text Books

Sr. No.	Title	Authors	Edition	Publisher
1	Computer Vision: Algorithms and Applications	Richard Szeliski	2nd	Springer Verlag London Limited.
2	Computer Vision: A Modern Approach	D. A. Forsyth, J. Ponce	2nd	Pearson Education

Reference Books

Sr. No.	Title	Authors	Edition	Publisher
1	Computer Vision: Models, Learning, and Inference	Simon J. D. Prince	2nd	Cambridge University

SEVEN SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
21AI703T(iv)	PE-IV AI for Cyber Security	3	-	-	3	30	70	100

Course Objectives	Course Outcomes
This course is intended to • The primary objective of this course is to equip AI engineering students with the knowledge and skills necessary to secure machine learning systems against various cyber threats. • Students will learn to identify and mitigate security risks in machine learning models, protect against adversarial attacks, and implement ethical practices in AI development.	**Students will be able to** • Learn the fundamental principles of machine learning security, including the different types of machine learning and their associated security risks. • Apply ethical considerations in machine learning tasks, ensuring data privacy, fairness, and user permission validation. • Detect and analyze anomalies in data to prevent malicious activities and employ effective anomaly detection strategies. • Develop methods to protect against ML-driven attacks, including the creation and detection of deepfakes and automated hacking techniques. • Apply ethical considerations in machine learning tasks, ensuring data privacy, fairness, and user permission validation.

Unit I - Securing a Machine Learning System	**[7Hrs]**
Defining Machine Learning Security : Defining Machine Learning Security, Building a picture of ML, Why is ML important?, Identifying the ML security domain, Understanding supervised learning, Understanding unsupervised learning, Understanding reinforcement learning, Distinguishing between supervised and unsupervised, Using ML from development to production. **Mitigating Risk at Training by Validating and Maintaining Datasets :** Technical requirements, Defining dataset threats, Detecting dataset modification, Mitigating dataset corruption. **Mitigating Inference Risk by Avoiding Adversarial Machine Learning Attacks:** Defining adversarial ML, Considering security issues in ML algorithms, Defining attacker motivations, Describing the most common attack techniques, Mitigating threats to the algorithm.	
Unit II - Creating a Secure System Using ML	**[8Hrs]**
Considering the Threat Environment: Technical requirements, defining an environment, understanding business threats, considering social threats, Employing ML in security in the real world. **Keeping Your Network Clean**: Defining current network threats, considering traditional protections, Adding ML to the mix, Creating real-time defenses.	
Unit III - Detecting and Analyzing Anomalies	**[7Hrs]**
Detecting and Analyzing Anomalies: Defining anomalies, Detecting data anomalies, Using anomaly detection effectively in ML, Considering other mitigation techniques. **Dealing with Malware :** Defining malware, Generating malware detection features, Classifying malware, Obtaining malware samples and labels.	
Unit IV - Protecting against ML-Driven Attacks	**[7Hrs]**
Considering the Ramifications of Deepfakes : Defining a deepfake, Creating a deepfake computer setup, Installing TensorFlow on a desktop system, Understanding autoencoders, Understanding CNNs and implementing GANs. **Leveraging Machine Learning for Hacking :** Making attacks automatic and personalized , Enhancing existing capabilities.	
Unit V - Performing ML Tasks in an Ethical Manner	**[8Hrs]**
Embracing and Incorporating Ethical Behavior : Sanitizing data correctly, Defining data source awareness, Validating user permissions, Understanding ML fairness, Determining what fairness means, Addressing fairness concerns, Mitigating privacy risks using federated learning and differential privacy, Distributing data and privacy risks using federated learning.	

Text Books

Sr. No.	Title	Authors	Edition	Publisher
1	Machine Learning Security Principles	John Paul Mueller	1st	Oreilly
2	Hands-On Artificial Intelligence for Cybersecurity	Alessandro Parisi	1st	Oreilly
3.	Machine Learning for Cybersecurity Cookbook	Emmanuel Tsukerman	1st	Oreilly

Reference Books

Sr. No.	Title	Authors	Edition	Publisher
1	Machine Learning Blueprints You Should Know for Cybersecurity	Rajvardhan Oak	1st	Oreilly
2	Hands-On Machine Learning for Cybersecurity	Soma Halder, Sinan Ozdemir	1st	Oreilly

Web Resources

https://www.packtpub.com/en-TH/product/machine-learning-security-principles-2-9781804618851/chapter/chapter-1-defining-machine-learning-security

https://www.packtpub.com/en-TH/product/machine-learning-security-principles-9781804618851#tocBlock

SEVEN SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
21AI703P(iv)	PE-IV AI for Cyber Security Lab	-	-	2	1	25	25	50

Course Objectives	Course Outcomes
This course is intended to • Quip AI engineering students with the knowledge and skills necessary to secure machine learning systems against various cyber threats. • Students will learn to identify and mitigate security risks in machine learning models, protect against adversarial attacks, and implement ethical practices in AI development.	**Students will be able to** • Learn the fundamental principles of machine learning security, including the different types of machine learning • Implement Supervise Algorithm using real time dataset. • Apply Unsupervised Algorithm for Facebook dataset • Use Validation to Mitigate risk • Develop methods to protect against ML-driven attacks, including the creation and detection of deepfakes and automated hacking techniques.

Sr. No.	List of Practicals
1	Write a program to perform a Linear Regression supervised Algorithm using Salary Dataset.
2	Write a program to perform a K-means Clustering Unsupervised Algorithm using Facebook Live Sellers in Thailand dataset.
3	Write a program to perform a Reinforcement learning using Q-Learning technique using Test hash dataset.
4	Write a program to perform a Mitigating Risk at Training by Validating and Maintaining Datasets. i. Write a program to implement detection of dataset modification. Write a program to implement Mitigating dataset corruption.
5	Develop a program to perform a Security in Machine Learning model in the Real-World example using i. Working with basic and digest authentication ii. A Simple spam filtering Manipulating filtered data (Word Pattern)
6	Construct a program to perform a Secure System Using ML (business threats, social threats) by the use of i. Stemming technique. Lemmatization technique.
7	Apply Random Forest classifier to perform a Secure System Using Machine Learning (real-time defenses).
8	Design a program to perform a Detection and Analyzation Anomalies i. Write a program to perform a detection of data anomalies (Checking data validity) using Interquartile Range (IQR). Write a program to perform an Analysis of Data Anomalies using Principal Component Analysis (PCA).
Open ended practical.	
9	Implement a program to perform a ML Tasks in an Ethical Manner. i. Write a program to perform a task of sanitizing data correctly. ii. Write a program to implement the concept of a Removing personally identifiable information. Write a program Eliminate unnecessary features.
10	Micro Project

Text Books

Sr. No.	Title	Authors	Edition	Publisher
1	Machine Learning Security Principles	John Paul Mueller	1st	Oreilly
2	Hands-On Artificial Intelligence for Cybersecurity	Alessandro Parisi	1st	Oreilly
3.	Machine Learning for Cybersecurity Cookbook	Emmanuel Tsukerman	1st	Oreilly

Reference Books

Sr. No.	Title	Authors	Edition	Publisher
1	Machine Learning Blueprints You Should Know for Cybersecurity	Rajvardhan Oak	1st	Oreilly
2	Hands-On Machine Learning for Cybersecurity	Soma Halder, Sinan Ozdemir	1st	Oreilly

Web Resources
https://www.packtpub.com/en-TH/product/machine-learning-security-principles-2-9781804618851/chapter/chapter-1-defining-machine-learning-security
https://www.packtpub.com/en-TH/product/machine-learning-security-principles-9781804618851#tocBlock

SEVEN SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
21AI704T(i)	PE-V AI in Health Care Domain	3	-	-	3	30	70	100

Course Objectives	Course Outcomes
This course is intended to • Learn the need and significance of AI and ML for Healthcare. • Study advanced AI algorithms for Healthcare. • Learn Computational Intelligence techniques. • Evaluate metrics and ethics in intelligence for Healthcare systems,	**Students will be able to** • Comprehend the role of AI and ML for handling Healthcare data • Apply Advanced AI algorithms for Healthcare Problems. • Apply various Computational Intelligence techniques for Healthcare Application. • Apply evaluation metrics for evaluating healthcare systems. • Develop NLP applications for healthcare using various NLP Techniques.

Unit I Introduction	**[7Hrs]**
Overview of AI , ML and DL,A Multifaceted Discipline, Applications of AI in Healthcare -Prediction, Diagnosis, personalized treatment and behavior modification, drug discovery, follow-up care etc,, Realizing potential of AI in healthcare, Healthcare Data - Use Cases.	
Unit II AI, ML, Deep Learning and Data Mining Methods for Healthcare	**[8Hrs]**
Knowledge discovery and Data Mining, ML, Multi classifier Decision Fusion, Ensemble Learning, Meta-Learning and other Abstract Methods. Evolutionary Algorithms, Illustrative Medical Application-Multiagent Infectious Disease Propagation and Outbreak Prediction, Automated Amblyopia Screening System etc. Computational Intelligence Techniques, Deep Learning, Unsupervised learning, dimensionality reduction algorithms.	
Unit III Evaluating learning for Intelligence	**[7Hrs]**
Model development and workflow, evaluation metrics, Parameters and Hyperparameters, Hyperparameter tuning algorithms, multivariate testing, Ethics of Intelligence.	
Unit IV Natural Language Processing in Healthcare	**[7Hrs]**
NLP tasks in Medicine, Low-level NLP components, High level NLP components, NLP Methods. Clinical NLP resources and Tools, NLP Applications in Healthcare. Model Interpretability using Explainable AI for NLP applications.	
Unit V Intelligent personal Health Record	**[7Hrs]**
Introduction, Guided Search for Disease Information, Recommending SCA's. Recommending HHP's , Continuous User Monitoring.	
Unit VI Future of Healthcare using AI	
Evidence based medicine, Personalized Medicine, Connected Medicine, Digital Health and Therapeutics, Conversational AI, Virtual and Augmented Reality, Blockchain for verifying supply chain, patient record access, Robot - Assisted Surgery, Smart Hospitals, Case Studies on use of AI and ML for Disease Risk Diagnosis from patient data, Augmented reality applications for Junior doctors. Blockchain for verifying supply chain, patient record access, Robot - Assisted Surgery, Smart Hospitals, Case Studies on use of AI and ML for Disease Risk Diagnosis from patient data, Augmented realitv applications for Junior doctors.	

Text Books

Sr. No.	Title	Authors	Edition	Publisher
1	Machine Learning and AI for Healthcare	Arjun Panesar	1st	A Press
2	Medical applications of Artificial Systems	Arvin Agah	1s	CRC Press

Reference Books

Sr. No.	Title	Authors	Edition	Publisher
1	Artificial Intelligence in Medical Imaging- Opportunities, Applications and Risks	Erik R. Ranschaert Sergey Morozov Paul R. Algra	5th	Springer
2	Data Science for Healthcare-Methodologies and Applications	Sergio Consoli Diego Reforgiato Recupero Milan Petković	2nd	Springer

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
21AI704T (ii)	PE-V AI in Finance Domain	3	-	-	3	30	70	100

Course Objectives	Course Outcomes
This course is intended to ● Comprehensive understanding of how artificial intelligence is revolutionizing the field of finance ● Focusing on the application of AI techniques to various financial tasks such as investment management, risk assessment, trading strategies, and fraud detection.	**Students will be able to** ● Learn basic concepts and applications of artificialintelligence in finance. ● Build machine learning algorithms and theirapplications in financial analysis. ● Apply practical skills in implementing AI techniques forfinancial modeling and prediction. ● Evaluate the impact of AI on financial markets andregulatory challenges. ● Explore ethical considerations and societalimplications of AI-driven finance.

Unit I Introduction to Artificial Intelligence in Finance	**[7Hrs]**
Overview of financial markets, instruments, and institutions, Introduction to artificial intelligence and machine learning, · Historicaldevelopments and recent trend, Applications of AI in finance: overview and potential impact, Ethical considerations and challenges in applying AI to finance.	
Unit II Data Preprocessing and Feature Engineering	**[7Hrs]**
Data collection and cleaning techniques for financial datasets, Feature engineering for financial modeling and prediction, Handling missing data, outliers, and data normalization, Time-series data preprocessing and feature extraction.	
Unit III Machine Learning Models in Finance	**[8 Hrs]**
Overview of supervised and unsupervised learning algorithms, Regression models for financial forecasting (e.g., stock price prediction), Classification models for fraud detection and credit risk assessment, Clustering techniques for portfolio optimization and customer segmentation, Predictive modeling for stock price forecasting and risk assessment.	
Unit IV Neural Networks and Deep Learning	**[7Hrs]**
Fundamentals of neural networks and deep learning, Architectures of deep learning models (e.g., feedforward neural networks, convolutional neural networks, recurrent neural networks). Applications of deep learning in finance: text mining, sentimentanalysis, and image recognition, Case studies of successful deep learning applications in finance	
Unit V AI Ethics and Regulation in Finance	**[7Hrs]**
Ethical considerations in AI-driven finance, Regulatory challenges and compliance requirements, Fairness, transparency, and accountabilityin AI algorithms, Societal implications and future directions	

Text Books

Sr. No.	Title	Authors	Edition	Publisher
1	Machine Learning for Finance: Principles and Applications in Python	Jannes Klaas	1st	Oreilly
2	Ethics of Artificial Intelligence and Finance"	Rajiv Sethi	1st	Oreilly
3.	Artificial Intelligence in Finance	Yves Hilpisch	1st	O'Reilly Media,

Reference Books

Sr. No.	Title	Authors	Edition	Publisher
1	Artificial Intelligence and Financial Markets	Lawrence R. Ritter	1st	Springer

ST. VINCENT PALLOTTI COLLEGE OF ENGINEERING & TECHNOLOGY, NAGPUR

(An autonomous institution affiliated to Rashtrasant Tukadoji Maharaj Nagpur University)

B. Tech. Scheme of Examination & Syllabus 2021-22

ARTIFICIAL INTELLIGENCE

SEVEN SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
21AI704T(iii)	PE-V AI in Agriculture Domain	3	-	-	3	30	70	100

Course Objectives	Course Outcomes
This course is intended to • Learn the basic principles and concepts of Artificial Intelligence (AI) and its relevance to the agricultural sector. • Implement precision agriculture techniques using AI to optimize inputs (water, fertilizers, and pesticides) and improve crop management.	**Students will be able to** • Comprehend AI and its usage in Agriculture domain. • Learn the basics of farming and how to use AI in agriculture domain. • Know the importance of water management and will learn its usage. • Automate various farming tasks with the use of AI domain. • Enhance the quality of food processing with the help of AI techniques like image processing, predictions etc.

Unit I : Introduction to AI for Agricultural	**[8Hrs]**
Basic concepts of Artificial Intelligence (AI), Artificial Neural Networks (ANNs), Machine Learning (ML), Machine Vision, Internet of Things (IoT), Cloud Computing, Statistical Computing, Deep Learning, Expert Systems, Automated Data Analytics.	
Unit II: AI for Agricultural Systems	**[7Hrs]**
Application of AI-ML for digital soil mapping, augmented reality for precise soil sampling, image processing for rapid soil property prediction via smartphone, soil spectroscopy-exploring the high dimensional soil spectral data, spectral preprocessing methods, modeling soil properties via ML algorithms, IoT in soil management.	
Unit III: AI for Water Management:	[7Hrs]
On-farm water, nutrient and pest management, crop damage assessment, decision support systems, crop modeling, smart irrigation, yield prediction, rainfall-runoff, streamflow, sediment and water quality.	
Unit IV: AI for Farm Mechanization	[7Hrs]
AI for Farm Mechanization: Application of AI for navigation of farm machinery, energy demand prediction for farm mechanization, and quality of tilth; Uniformity prediction for sowing, planting and transplanting; Crop disease detection, quantification of severity and mitigation; crop yield monitoring, and prediction of harvesting and threshing quality; AI for farm machinery management and custom hiring.	
Unit V: AI for Food Processing	[7Hrs]
Application of AI and ML in food processing and packaging. Non-destructive quality evaluation of food based on spectral data, Image based quality detection, varietal identification of fruits and vegetables, sorting of products and packages, decision making for the consumers and profit enhancement by the industry people by proper market survey using AI, new product formulation.	

Text Books

Sr.No.	Title	Authors	Edition	Publisher
1	Agricultural Mechanization and Automation	Paul McNulty, Patrick M. Grace	2nd	Eolss Publishers
2	Innovations in Machine Learning and IoT for Water Management	Kumar, Abhishek, Srivastav, Arun Lal, Dubey, Ashutosh Kumar	1st	IGI Global
3.	Agriculture 5.0 Artificial Intelligence, IoT and Machine Learning	Latief Ahmad, Firasath Nabi	1st	CRC Press
4.	AI in Food Industry for Food Products Quality Inspection	Dr Syeda Sumera Ali	1st	Blue Rose Publishers

Reference Books

Sr.No.	Title	Authors	Edition	Publisher
1	Hands-On Artificial Intelligence for IoT	Amita Kapoor	1st	Oreilly
2	Internet of Things and Analytics for Agriculture	Prasant Kumar Pattnaik, Raghvendra Kumar, Souvik Pal	3rd	Springer

ST. VINCENT PALLOTTI COLLEGE OF ENGINEERING & TECHNOLOGY, NAGPUR

(An autonomous institution affiliated to Rashtrasant Tukadoji Maharaj Nagpur University)

B. Tech. Scheme of Examination & Syllabus 2021-22

ARTIFICIAL INTELLIGENCE

SEVEN SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
21AI761O (i)	OE-III Introduction to Cloud Computing with ML	3	-	-	3	30	70	100

Course Objectives	Course Outcomes
This course is intended to • Understand the Machine Learning Workflow • Leverage AWS Services for ML • Hands-On Practical Experience • Focus on Model Deployment and Management	**Students will be able to** • Introduction to cloud and machine learning concepts. • Interpret machine learning on AWS and data preparation. • Perform exploratory data analysis in AWS. • Apply Model Selection, training, evaluation and hyper parameter tuning in AWS cloud. • Learn Deploying, monitoring and managing ML Models on AWS

Unit I: Introduction to cloud and machine learning	**[7Hrs]**
Definition and Evolution of Cloud Computing, Cloud Service Models: IaaS, PaaS, SaaS, Cloud Deployment Models: Public, Private, Hybrid, Community, virtualization, virtual machine concept, Overview of Major Cloud Service Providers. Overview of machine learning concepts, definition, types of machine learning, applications. Machine learning algorithms: Supervised algorithms: Regression, classification: KNN, Naïve bayes, decision trees, random forest, SVM. Unsupervised algorithms: k-means, DBSCAN, hierarchical clustering algorithms.	
Unit II: Introduction to Machine Learning with AWS	**[8Hrs]**
AWS Services for Machine Learning, Setting Up Your AWS Environment, Introduction to Amazon SageMaker, **Data Preparation for Machine Learning** Data Collection Strategies, Data Cleaning and Preprocessing, Data Storage on AWS: S3, RDS, DynamoDB, Hands-On: Uploading and Managing Data on AWS.	
Unit III: Exploratory Data Analysis in AWS	**[7Hrs]**
Techniques for EDA, Visualizing Data with AWS Services, Hands-On: EDA using AWS Glue and Amazon QuickSight.	
Unit IV: Model Selection, training, evaluation and hyperparameter tuning	**[7Hrs]**
Choosing the Right Model, Training Machine Learning Models, Distributed Training on AWS, Hands-On: Training a Model with Amazon SageMaker, Evaluating Model Performance, Hyperparameter Tuning Techniques, Using SageMaker for Hyperparameter Optimization, Hands-On: Hyperparameter Tuning on AWS	
Unit V: Deploying, monitoring and managing ML Models on AWS	**[7Hrs]**
Introduction to Model Deployment, Deploying Models with SageMaker Endpoints, Hands-On: Deploying a Model to Production on AWS, Model Monitoring and Logging, Managing Model Versions, Hands-On: Monitoring and Managing Models with SageMaker, Case Study: Healthcare, Finance, and Retail.	

Text Books

Sr. No.	Title	Authors	Edition	Publisher
1.	Cloud Computing: Concepts, Technology & Architecture	Thomas Erl	1st	Prentice Hall

		July 2024	1.3	Applicable for 2024-25
Chairman - BoS	Dean – Academics	Date of Release	Version	

2.	Practical Machine Learning with AWS: Process, Build, and Deploy Intelligent Solutions	Himanshu Singh and Drew Tawse	1st	O'Reilly
3.	Architecting the Cloud: Design Decisions for Cloud Computing Service Models	Michael J. Kavis	1st	Wiley

Reference Books

Sr. No.	Title	Authors	Edition	Publisher
1.	Mastering Cloud Computing: Foundations and Applications Programming	Rajkumar Buyya, Christian Vecchiola, and S. Thamarai Selvi	1st Edition	Morgan Kaufmann
2.	Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow	Aurélien Géron	2nd Edition	O'Reilly Media

ST. VINCENT PALLOTTI COLLEGE OF ENGINEERING & TECHNOLOGY, NAGPUR

(An autonomous institution affiliated to Rashtrasant Tukadoji Maharaj Nagpur University)

B. Tech. Scheme of Examination & Syllabus 2021-22

ARTIFICIAL INTELLIGENCE

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
21AI761O (ii)	OE-III Ethical Hacking	3	-	-	3	30	70	100

Course Objectives	Course Outcomes
This course is intended to • Evaluate the security policies and identify vulnerabilities in target systems, networks or system infrastructure. • Introduce the methodologies and framework of ethical hacking for enhancing the security.	**Students will be able to** • Learn the basics of ethical hacking and malware. • Evaluate the concept of planning for controlled attack. • Demonstrate the concept of Preparing for a hack • Apply the concept of enumeration and exploitation. • Demonstrate the concept of Deliverable and Integration

Unit I Introduction to Ethical Hacking	**[8 Hrs]**
Introduction: Hacking Impacts, The Hacker Framework: Planning the test, Sound Operations, Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Final Analysis, Deliverable, Integration Information Security Models: Computer Security, Network Security, Service Security, Application Security, Security Architecture Information Security Program: The Process of Information Security, Component Parts of Information Security Program, Risk Analysis and Ethical Hacking.	
Unit II Planning for a Controlled Attack	**[8 Hrs]**
The Business Perspective: Business Objectives, Security Policy, Previous Test Results, Business Challenges Planning for a Controlled Attack: Inherent Limitations, Imposed Limitations, Timing is Everything, Attack Type, Source Point, Required Knowledge, Multi-Phased Attacks, Teaming and Attack Structure, Engagement Planner, The Right Security Consultant, The Tester, Logistics, Intermediates, Law Enforcement	
Unit III Preparing for a Hack	**[7 Hrs]**
Preparing for a Hack: Technical Preparation, Managing the Engagement Reconnaissance: Social Engineering, Physical Security, Internet Reconnaissance	
Unit IV Enumeration and Exploitation	**[7 Hrs]**
Enumeration: Enumeration Techniques, Soft Objective, Looking Around or Attack, Elements of Enumeration, Preparing for the Next Phase Exploitation: Intuitive Testing, Evasion, Threads and Groups, Operating Systems, Password Crackers, Rootkits, applications, Wardialing, Network, Services and Areas of Concern	
Unit V Deliverable and Integration	**[7 Hrs]**
Deliverable: The Deliverable, The Document, Overall Structure, Aligning Findings, Presentation Integration: Integrating the Results, Integration Summary, Mitigation, Defense Planning, Incident Management, Security Policy, Conclusion	

Text Books

Sr. No.	Title	Authors	Edition	Publisher
1.	The Ethical Hack: A Framework for Business Value Penetration Testing	James S. Tiller	1st	Auerbach Publications
2.	The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy	Patrick Engebretson.	2nd	Syngress
3	Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives.	Sunit Belapure and Nina Godbole	1st	Wiley India

Reference Books

Sr. No.	Title	Authors	Edition	Publisher
1	CEH official Certified Ethical Hacking Review Guide	Kimberly Graves	2nd	Willey
2	Hands-On Ethical Hacking and Network Defense"	Michael Simpson, Kent Backman, James Corley	1st	Cengage Learning

		July 2024	1.3	Applicable for 2024-25
Chairman - BoS	Dean – Academics	Date of Release	Version	