



**D Y PATIL**  
**INTERNATIONAL**  
**UNIVERSITY**  
AKURDI PUNE

# *Advanced AI*



**Dr. Vaishnav G. Kale**  
**Associate Professor**

**Department of Computer Science**  
**Engineering & Applications**

**D.Y. Patil International University, Pune**

# About the Course

Name of the subject:Advanced AI

Course Code:MCA 301

Programme:Master in Computer Applications

Year of study:Second Year

Semester :III

Specialization:Artificial Intelligence and Data Science

Course Type:Specialization Course

Academic Year:2023-24

# Syllabus

## **Module-V:Emerging Trends in AI**

- Introduction to Computer Vision and its Applications
- Introduction to Natural Language Processing and its Applications
- Introduction to Explainable AI and Interpretability
- Introduction to Quantum AI and its potential impact
- Introduction to Edge AI and Federated Learning

# Books

Sr.No.	Text Books	Name of the Author
1	“Artificial Intelligence: A Modern Approach”	Stuart Russell and Peter Norvig
2	“A First Course in Artificial Intelligence”	Deepak Khemani
3	“Artificial Intelligence”	Elaine Rich, Kevin Knight and Nair
4	“Deep Learning”	Ian Goodfellow The MIT Press
Sr.No.	Reference Books	Name of the Author
1	“Artificial Intelligence: A new Synthesis”	Nilsson Nils J
2	“Artificial Intelligence”	Patrick Henry Winston
3	“Computational Intelligence: An Introduction”	Andries P. Engelbrecht
4	“Artificial Intelligence: Concepts and Applications”	Dr. Lavika Goel

# Advanced Artificial Intelligence

## Module 05. Emerging Trends in AI

# Computer Vision






- One of the most powerful and compelling types of AI is computer vision
- Computer vision is the field of computer science that focuses on replicating parts of the complexity of the human vision system and enabling computers to identify and process objects in images and videos in the same way that humans do.
- One of the driving factors behind the growth of computer vision is the amount of data we generate today that is then used to train and make computer vision better.
- Along with a tremendous amount of visual data (*more than 3 billion images are shared online every day*), the computing power required to analyze the data is now accessible.
- As the field of computer vision has grown with new hardware and algorithms so has the accuracy rates for object identification.



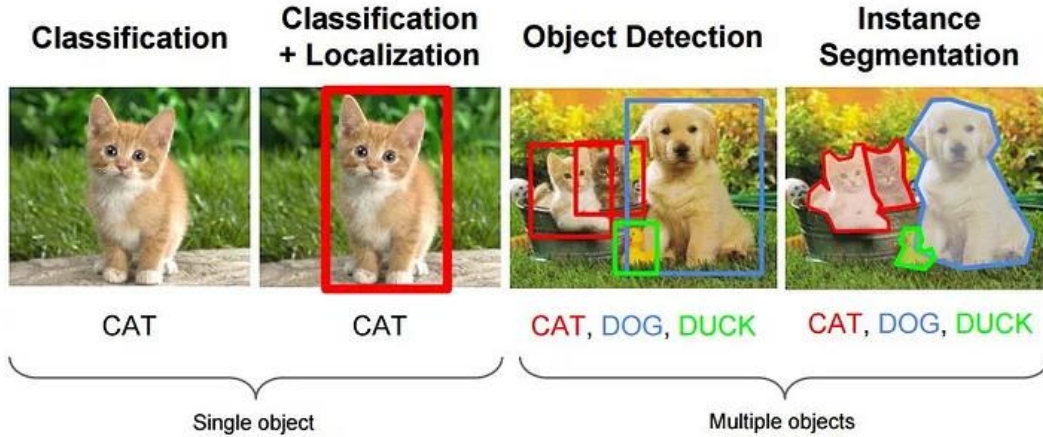
## How to create colors with RGB?

Combine parts of the three primary colors **red**, **green** and **blue**.

Each of the primary colors can have a value in the range from 0 to 255.

					
R:	255	0	0	0	255
G:	0	255	0	0	255
B:	0	0	255	0	255

## Computer Vision Tasks



## Applications

- 1) Self Driving Cars
- 2) Facial Recognition
- 3) Augmented Reality and Mixed Reality
- 4) Health care



# Computer Vision

- **Object Classification:** What broad category of object is in this photograph?
- **Object Identification:** Which type of a given object is in this photograph?
- **Object Verification:** Is the object in the photograph?
- **Object Detection:** Where are the objects in the photograph?
- **Object Landmark Detection:** What are the key points for the object in the photograph?
- **Object Segmentation:** What pixels belong to the object in the image?
- **Object Recognition:** What objects are in this photograph and where are they?

# Computer Vision

Outside of just recognition, other methods of analysis include:

- **Video motion analysis** uses computer vision to estimate the velocity of objects in a video, or the camera itself.
- In **image segmentation**, algorithms partition images into multiple sets of views.
- **Scene reconstruction** creates a 3D model of a scene inputted through images or video.
- In **image restoration**, noise such as blurring is removed from photos using Machine Learning based filters.

Any other application that involves understanding pixels through software can safely be labeled as computer vision.

# Natural Language Processing

- Natural language processing is the artificial intelligence-driven process of making human input language decipherable to software.
- Natural language processing (NLP) is the capacity of computer software to interpret spoken and written human language, often known as natural language.

## Terms

- **NLP:** (Natural Language Processing) is in charge of processes such as decisions and actions.
- **NLU:** (**Natural Language Understanding**) understands the meaning of the text.
- **NLG:** (Natural Language Generation) creates the human language text from the structured data that the system generates to answer.

# Natural Language Processing

- Several NLP tasks break down human text and voice data in ways that help the computer make sense of what it's ingesting. Some of these tasks include the following:

## 1) **Speech recognition**

- Also called speech-to-text, is the task of reliably converting voice data into text data.
- Speech recognition is required for any application that follows voice commands or answers spoken questions.
- What makes speech recognition especially challenging is the way people talk—quickly, slurring words together, with varying emphasis and intonation, in different accents, and often using incorrect grammar.

## 2) **Part of speech tagging(grammatical tagging)**

- It is the process of determining the part of speech of a particular word or piece of text based on its use and context.

# Natural Language Processing

## 3) Word Sense Disambiguation(WSD)

- It is the selection of the meaning of a word with multiple meanings through a process of semantic analysis that determine the word that makes the most sense in the given context.

## 4) Named entity recognition(NEM)

- Identifies words or phrases as useful entities.

## 5) Co-reference resolution

- It is the task of identifying if and when two words refer to the same entity.
- The most common example is determining the person or object to which a certain pronoun refers (e.g., 'she' = 'Mary')

## 6) Sentiment analysis

- It attempts to extract subjective qualities—attitudes, emotions, sarcasm, confusion, suspicion—from text.

# Natural Language Processing

## **Preprocessing of the Text using NLTK**

- 1) Sentence Parsing
- 2) Word Segmentation
- 3) Stemming and Lemmatization (methods of trimming words down to their roots),
- 4) Tokenization (for breaking phrases, sentences, paragraphs and passages into tokens that help the computer better understand the text).
- 5) Change case
- 6) Spell Correction
- 7) Stop Words Removal
- 8) Text Normalization
- 9) It also includes libraries for implementing capabilities such as semantic reasoning, the ability to reach logical conclusions based on facts extracted from text.

# NLP Use cases

## 1) Spam Detection

- spam detection technologies use NLP's text classification capabilities to scan emails for language that often indicates spam or phishing.
- These indicators can include overuse of financial terms, characteristic bad grammar, threatening language, inappropriate urgency, misspelled company names, and more.

## 2) Machine Translation

- Google Translate is an example of widely available NLP technology at work.
- Truly useful machine translation involves more than replacing words in one language with words of another.
- Effective translation has to capture accurately the meaning and tone of the input language and translate it to text with the same meaning and desired impact in the output language.
- Machine translation tools are making good progress in terms of accuracy.

# NLP Use cases

## 3) Virtual agents and chatbots:

- **Virtual agents** such as Apple's Siri and Amazon's Alexa use speech recognition to recognize patterns in voice commands and natural language generation to respond with appropriate action or helpful comments.
- **Chatbots** perform the same magic in response to typed text entries.
- The best of these also learn to recognize contextual clues about human requests and use them to provide even better responses or options over time.
- The next enhancement for these applications is question answering, the ability to respond to our questions—anticipated or not—with relevant and helpful answers in their own words.



# NLP Use cases

## 4) Social media sentiment analysis:

- NLP has become an essential business tool for uncovering hidden data insights from social media channels.
- Sentiment analysis can analyze language used in social media posts, responses, reviews, and more to extract attitudes and emotions in response to products, promotions, and events—information companies can use in product designs, advertising campaigns, and more.

## 5) Text summarization:

- Text summarization uses NLP techniques to digest huge volumes of digital text and create summaries and synopses for indexes, research databases, or busy readers who don't have time to read full text.
- The best text summarization applications use semantic reasoning and natural language generation (NLG) to add useful context and conclusions to summaries.

# Explainable AI (XAI)

- Explainable AI refers to the concept of how AI works and how it arrives at those decisions being made clear to humans.
- Explainable AI is concerned with explaining input variables and the decision-making stages of a model.
- It is also concerned with the structure of the models themselves.
- Explainable AI would help reduce incidents of bias.
- The algorithms would be fine-tuned to provide better and fairer experiences to all users.
- To develop explainable systems, two main techniques are used; *ante-hoc* and *post-hoc*.

# Explainable AI (XAI)

## 1) Ante-Hoc Methods

- These techniques involve implementing explainability into an AI model from the very beginning.

### a) Reverse Time Attention Model (RETAIN)

- To assist doctors with understanding AI software predictions, the RETAIN model was developed.
- It utilizes two recurrent neural networks, each having an attention mechanism.
- The attention mechanism was responsible for explaining the focus of the neural network and how a choice was influenced.

### b) Bayesian Deep Learning (BDL)

- BDL is a field that combines the Bayesian probability theory and deep learning architectures.
- With BDL, it's possible to measure the unreliability within the predictions of a neural network.
- Bayesian deep learning models usually form prediction uncertainty estimates, that assist in describing features that led to certain decisions being made.

# Explainable AI (XAI)

## 2) Post-Hoc Methods

- These techniques only involve explainability during testing stages.
- The training stages are carried out normally.
- Post-hoc model analysis is a very common approach towards explaining AI in production.

### a) **Local interpretable Model-Agnostic Explanations (LIME)**

- LIME receives input, then generates a new dataset composed of refined data samples.
- The next step involves populating corresponding predictions that would have been made by a black-box model if the aforementioned samples would have been used as input.
- Next is the training of an interpretable model (such as regression models or decision trees).
- The model is trained on the new dataset to help explain changes in the key extracted features.

# Explainable AI (XAI)

## 2) Post-Hoc Methods

### b) Black Box Explanation through Transparent Approximation (BETA)

- BETA is a post hoc method that is linked to Interpretable Decision Sets.
- **Interpretable Decision Sets** is a framework used to build highly accurate and interpretive predictive models.
- Interpretable Decision Sets generate interpretable classification models for multi-class classification tasks.
- They do this without significantly sacrificing accuracy.
- These decision sets are sets of “if-then” rules.
- These rules are not connected by “else” statements and can be considered in any order.
- Each rule exists as an independent classifier.

# Explainable AI (XAI)

## Challenges to Achieving XAI

- 1) Different users, different levels of explainability, different contexts
- 2) Performance-explainability trade-off
  - There exists an **inverse relationship** between AI method accuracy and interpretability.
  - The greater the accuracy, the lower the interpretability.
  - This means that the lower the accuracy, the higher the interpretability.
- 3) Explainability-privacy trade-off
- 4) Malicious actors
  - If a system offers seemingly transparent yet inaccurate explanations of its inner workings, it would be hard for most users to tell.
  - This could motivate malicious actors to deceive users into believing they offer explainability while not being the case. This could lead to users being easily exploited yet never suspecting it.

# Quantum AI and its Potential Impact

- Quantum computing is a new paradigm in computing that leverages the principles of quantum mechanics to perform calculations that are impossible or infeasible for classical computers.
- Unlike classical computers, which use bits to represent information as 0s and 1s, quantum computers use quantum bits, or qubits, which can represent information as both 0 and 1 simultaneously.
- This property, known as superposition, allows quantum computers to perform many calculations at once, potentially solving complex problems much faster than classical computers.
- Quantum computers could potentially revolutionize AI by providing a more efficient way to train machine learning models and solve optimization problems.
- For instance, quantum computers could be used to train deep learning models much faster than classical computers, enabling AI researchers to explore larger and more complex models.

# Quantum AI and its Potential Impact

## The Impact of Quantum Computing on Artificial Intelligence

- Quantum computing boosts the potential of AI by amplifying its velocity, efficacy, and precision.
- Utilizing qubits and capitalizing on non-linear operations
- Let's explore the impact of quantum computing on different industries and the transformative effects it brings to AI-driven processes.

### 1) Medical Care

- By inputting various possibilities and relevant historical data, **healthcare** professionals can leverage quantum computing to evaluate treatment effectiveness and receive optimal recommendations swiftly.

### 2) Machine Learning

- Quantum computing comes into play, offering the potential to rapidly process large volumes of data rapidly, thus granting machine learning the same advantage.



# Quantum AI and its Potential Impact

## 3) Cryptography and Security

- Quantum computing can make it harder for unauthorized parties to breach data using qubits to calculate all possible breach methods, allowing for stronger security measures.

## 4) Financial Applications

- Quantum computing's integration promises to enhance market predictions and risk management.

## 5) Natural Language Processing

- Quantum computing can enhance **natural language processing** (NLP) and speech recognition, leading to more efficient and accurate communication.
- In that sense, quantum NLP (QNLP) aims to surpass the capabilities of traditional NLP by translating language into coded circuits processed by quantum computers.
- Through the transformation of sentences into logical formats and the use of string diagrams, QNLP simplifies NLP design on quantum hardware.
- These encoded quantum circuits can be optimized for machine learning applications.

# Quantum AI and its Potential Impact

## Advantages

- 1) The ability of quantum computing to process vast amounts of data at an astonishing speed is of utmost importance when it comes to tackling intricate problems.
- 2) Optimizing the solutions
- 3) Spotting Patterns/anomalies in the vast, unsorted dataset
- 4) Facilitating Integration of Diverse Data Sets

# Quantum AI and its Potential Impact

## Challenges

### 1) Qubit decoherence:

- The loss or degradation of quantum information in a qubit, stands as one of the most significant hurdles in the realm of quantum computing. These qubits are incredibly sensitive to their surroundings, meaning even minor disruptions can lead to the loss of their quantum properties.

### 2) Error Correction:

- Quantum computers prove highly susceptible to noise and errors resulting from interactions with the environment.

### 3) Scalability :

- Although quantum computers have shown remarkable capabilities in specific areas, their current size and scale still fall short when compared to classical computers.

# Quantum AI and its Potential Impact

## **4) Hardware Development:**

- The development of high-quality quantum hardware, including qubits and control electronics, presents a significant obstacle.

## **5) Software Development:**

- Quantum algorithms and software development tools are currently in their early stages, necessitating the creation of new programming languages, compilers, and optimization tools.

## **6) Interface with Classical Computers:**

- Quantum computers are not intended to replace classical computers; instead, they will serve as complementary technologies.

## **7) Trained Talent**

## **8) Overall Expense**

# Edge AI

- Edge AI is the implementation of artificial intelligence in an edge computing environment.
- That means AI computations are done at the edge of a given network, usually on the device where the data is created — like a camera or car — instead of in a centralized cloud computing facility or offsite data center.
- For example, let's say you have a smart coffee pot that can produce custom drinks for each user
- But unlike most smart devices, this coffee pot isn't connected to the internet and all of the algorithms it uses to process data are generated within the coffee pot itself .....this is edge AI.
- Edge AI's ability to more securely produce **real-time analytics** at higher speeds, lower costs and with less power has made it an attractive alternative to cloud computing AI

Put simply, edge AI is a combination of edge computing and artificial intelligence.

## Edge computing

- Edge computing is a distributed computing framework that brings computations and data storage closer to actual devices rather than off-site data centers.
- These days, **smart devices** are everywhere. Everything from the watch on your wrist to the car in your garage is capable of performing autonomous computing and exchanging data with other smart devices — a concept commonly known as the **internet of things**, or IoT.
- All that data flying back and forth puts a heavy strain on data centers. But edge computing is meant to ease that burden by moving some of the processing closer to its point of origin. So, rather than traveling to **the cloud**, the job is done on “on the edge”.
- The “edge” simply refers to the device being used. This can be a phone, a camera, a car, a medical device or a television. So edge computing is when the computer is inside or near that device

# Edge AI

## Edge AI

- Putting it all together, edge AI is essentially “doing that work and making decisions locally
- It’s the processing, it’s gathering the data, it’s understanding the data — not in big servers or in the cloud, but in your house, in a work or a job site, or in a parking garage
- “It’s about moving the different mathematical algorithms, and running those predictions at the edge.”
- With edge AI, **algorithms** can run directly at the edge of a given network, close to where the data and information needed to run the system are generated, such as an IoT device or machine equipped with an edge computing device.
- Edge AI devices use embedded algorithms to monitor the device’s behavior, as well as collect and process the device data. This allows the device to make decisions, automatically correct problems and make future performance predictions.

# Edge AI

## Edge AI

- Edge AI can run on a wide range of **hardware**, from existing central processing units, or CPUs, to microcontrollers and advanced neural processing devices.

## Edge AI Vs Cloud AI

- Cloud AI is when data is processed and stored on the cloud.
- This offers software engineers more flexibility in the design and structure of cloud AI systems, but it requires an internet connection to function.
- Cloud AI's dependence on internet connectivity can potentially lead to efficiency and security issues.
- Since edge AI processes and stores data locally and without internet connection, the technology can produce real-time data and make independent decisions.



## Examples of Edge AI

### 1) Health Monitoring Devices

- All the data collected from **health monitoring devices** like cardiac trackers and blood pressure sensors can be processed and analyzed locally, enabling real-time analytics that help medical professionals provide better care to patients.

### 2) Self Driving Cars

- When a 4,000-pound autonomous vehicle is driving down a busy road, every millisecond counts.
- The rapid data processing enabled by edge AI allows the system to respond quickly to the world around it — ideally making it a safer, more reliable contraption.

## Examples of Edge AI

### 3) Security Cameras

- Edge AI's use of computer vision, object detection and facial recognition makes some security cameras, like ones from [Vmukti](#), particularly effective.
- They allow for two-way audio, digital zoom and remote monitoring from any location.

### 4) Smart Homes

- From video doorbells to voice controlled light bulbs and refrigerators that monitor things like food consumption and expiration dates, [smart homes](#) contain a web of IoT devices that are meant to work together
- Instead of these devices having to send all the data from the house to a centralized remote server for processing, edge AI allows all of this to happen onsite, making it faster and more secure.

# Federated Learning

- Federated learning is a way to train AI models without anyone seeing or touching your data, offering a way to unlock information to feed new AI applications.
- Many of these AI applications were trained on data gathered and crunched in one place. But today's AI is shifting toward a decentralized approach.
- New AI models are being trained collaboratively on the edge on data
- This new form of AI training is called federated learning, and it's becoming the standard for meeting a raft of new regulations for handling and storing private data.
- By processing data at their source, federated learning also offers a way to tap the raw data streaming from sensors and smart devices.

# Federated Learning

- Under federated learning, multiple people remotely share their data to collaboratively train a single deep learning model, improving on it iteratively, like a team presentation or report.
- Each party downloads the model from a datacenter in the cloud, usually a pre-trained **foundation model**.
- They train it on their private data, then summarize and encrypt the model's new configuration.
- The model updates are sent back to the cloud, decrypted, averaged, and integrated into the centralized model. Iteration after iteration, the collaborative training continues until the model is fully trained.

# Federated Learning

- This distributed, decentralized training process comes in three flavors.
- In horizontal federated learning, the central model is trained on similar datasets.
- In vertical federated learning, the data are complementary; movie and book reviews, for example, are combined to predict someone's music preferences.
- Finally, in federated transfer learning, a pre-trained foundation model designed to perform one task, like detecting cars, is trained on another dataset to do something else, like identify cats.
- To make useful predictions, deep learning models need tons of training data. But companies in heavily regulated industries are hesitant to take the risk of using or sharing sensitive data to build an AI model for the promise of uncertain rewards.
- Federated learning could allow companies to collaboratively train a decentralized model without sharing confidential medical records.

# Federated Learning

## Challenges

- 1) Training AI models collaboratively, in multiple places at once, is computationally intensive. It also requires high communication bandwidth.
- 2) Transparency is another challenge for federated learning. Because training data are kept private, there needs to be a system for testing the accuracy, fairness, and potential biases in the model's outputs
- 3) Another challenge for federated learning is controlling what data go into the model, and how to delete them when a host leaves the federation. Because deep learning models are opaque, this problem has two parts: finding the host's data, and then erasing their influence on the central model.
- 4) A final challenge for federated learning is trust. Not everyone who contributes to the model may have good intentions.

# Thank you!



**D Y PATIL**  
**INTERNATIONAL**  
**UNIVERSITY**  
AKURDI PUNE