Applied AI & ML Industry Projects Lab (AAM-IPL)
Transforming Learning into Industry Solutions

Inaugural Lecture

Introduction and State of the Art in AI & ML

V Semester - ML and AIUP, Aug-Oct 2024

Session Date and Time: 8th Sept 2024, 10:30 AM IST – 12:00 Noon IST

Venkateswar Reddy Melachervu
Visiting Faculty and CTO, Brillium Technologies
Department of Computer Science Engineering – AI and ML (CSM)
Email: venkat.reddy.gf@gprec.ac.in

G.Pulla Reddy Engineering College (Autonomous)
G.Pulla Reddy Nagar, Nandyal Road, Kurnool, AP 518007, India
Website: https://www.gprec.ac.in

Disclaimer and Confidentiality Notice

The content of this guest lecture, including all discussions, materials, and demonstrations, is intended for educational purposes only and reflects the views and opinions of the speaker. While every effort has been made to ensure the accuracy and relevance of the information presented, it should not be considered as legal, financial, or professional advice.

Brillium Technologies retains unrestricted ownership of all information shared during this session. Participants must not record, reproduce, distribute, or disclose any part of the lecture or materials without prior written permission from Brillium Technologies. Unauthorized use or distribution of the content may result in legal action.

Additionally, all trademarks, service marks, and intellectual properties referenced or used in this presentation are the property of their respective owners. No ownership or rights over such third-party content are claimed or implied by the author or Brillium Technologies.

By attending this lecture, you agree to respect the confidentiality of the information shared and refrain from using it in any unauthorized manner. Failure to comply with these terms may result in legal action.

Thank you for your understanding and cooperation.

Lecture Outline

- What is AI & ML
- The Universe of AI, ML, DS
- AI Capabilities, Types, Sub-fields, Core Areas, Layer Hierarchy
- Real-world AI Applications
- How Do Machines Learn?
- AI Key Concepts
- AI Timeline and 21st Century Growth Enablers
- GPTs and LLMs Key Concepts
- State of the Art in AI & ML
- Dangers, Challenges and Limitations of AI
- Future Direction of AI
- AAM-IPL Overview
- Q&A
- Call to Action

What is AI?

This image is created (2 iterations) by Google Gemini's Imagen 3 for this presentation.
The prompt provided is "A central image of a brain merging with a digital network (to represent the fusion of human intelligence and artificial intelligence)."

What makes machines *think*?

- Can machines understand language like we do?
- How do algorithms recognize faces and voices?
- What powers the creativity of AI-generated art?
- Is AI just a tool, or could it ever be more?

Artificial Intelligence is the New Electricity!

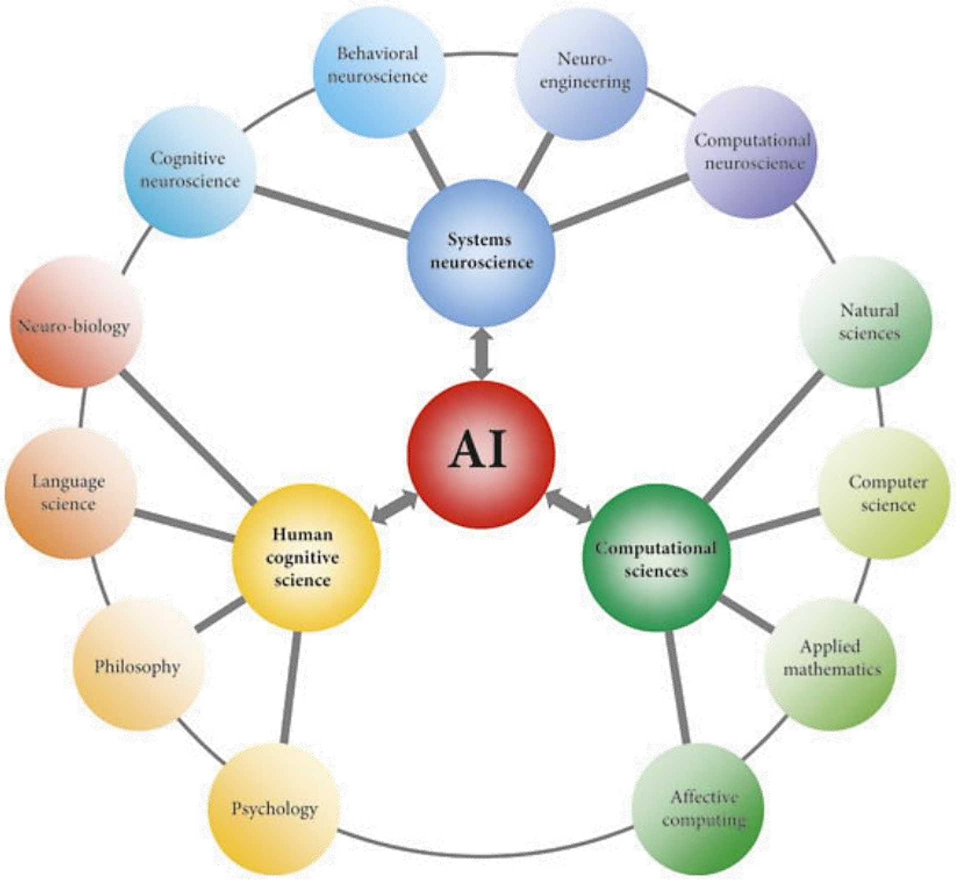
- Andrew Ng, AI Pioneer, Adjunct Professor at Stanford University, Co-founder and Chairman of Coursera

AI – Multi-disciplinary Science

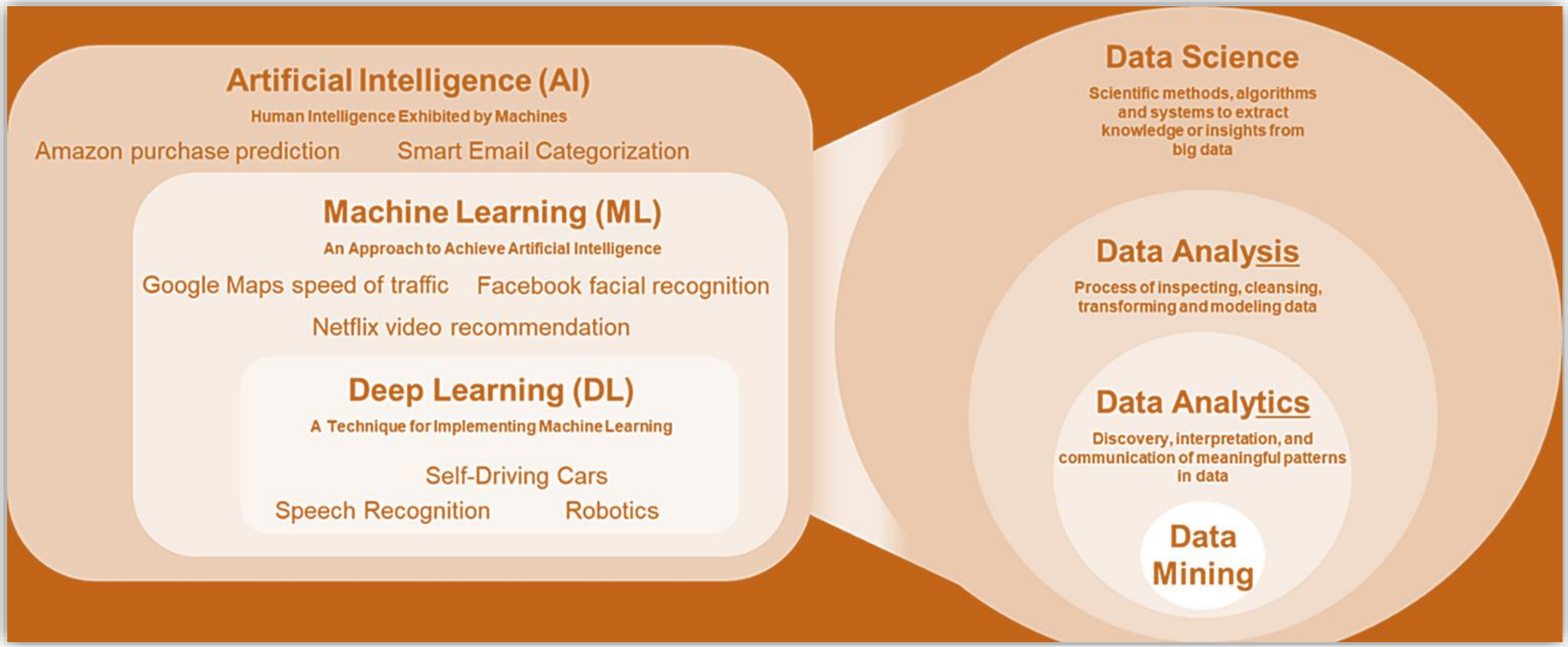
Branch of computer science and engineering and intersection of many other sciences

- Mimic human cognitive functions - such as learning, problem-solving, and decision-making

- Learn, reason, solve real-life or business problems, perceive things, understand natural languages like English, make decisions etc.

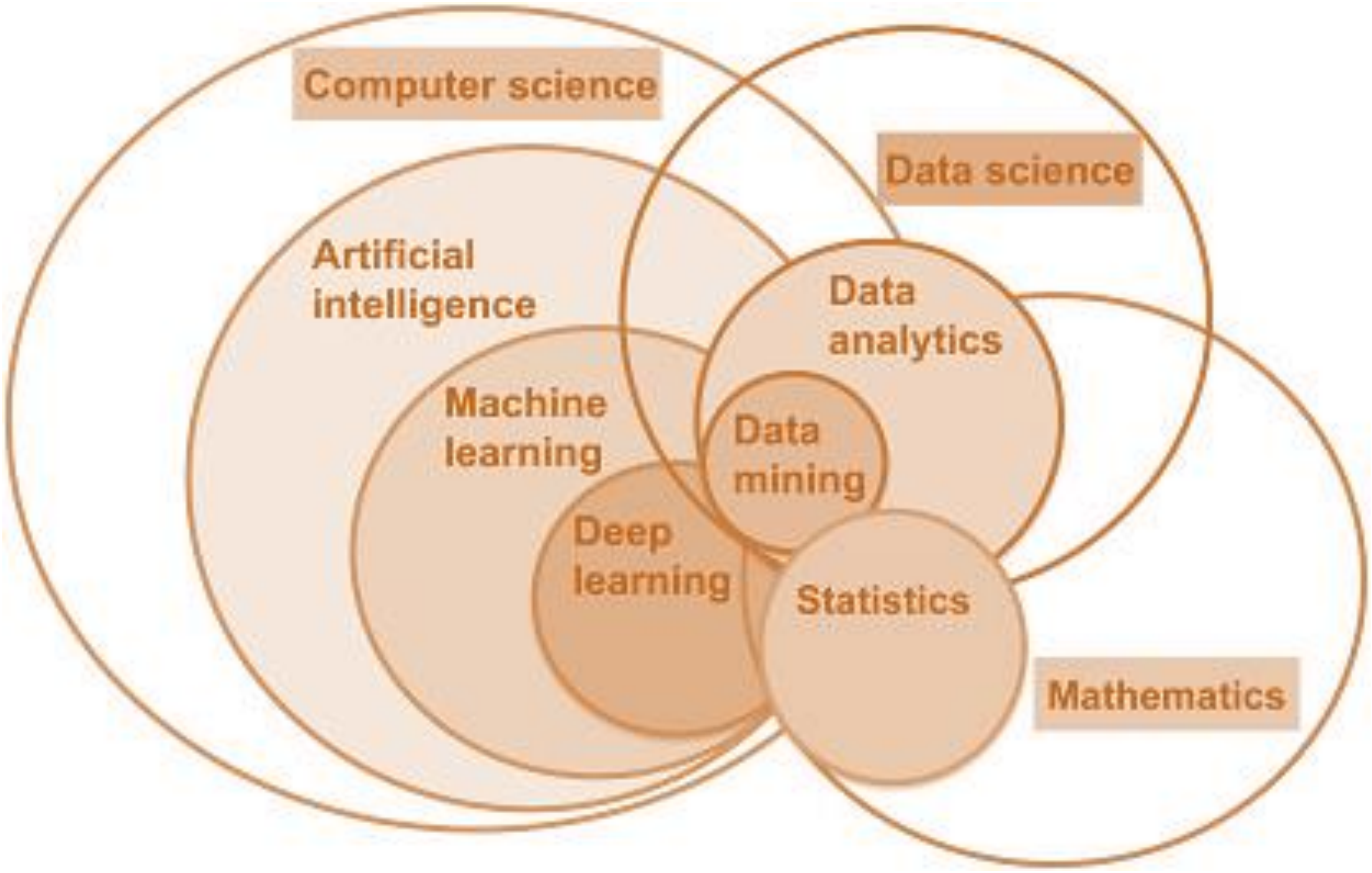


The Universe of Data Science and Artificial Intelligence



Big Data

The AI Intersection of Sciences



AI Capabilities and Types

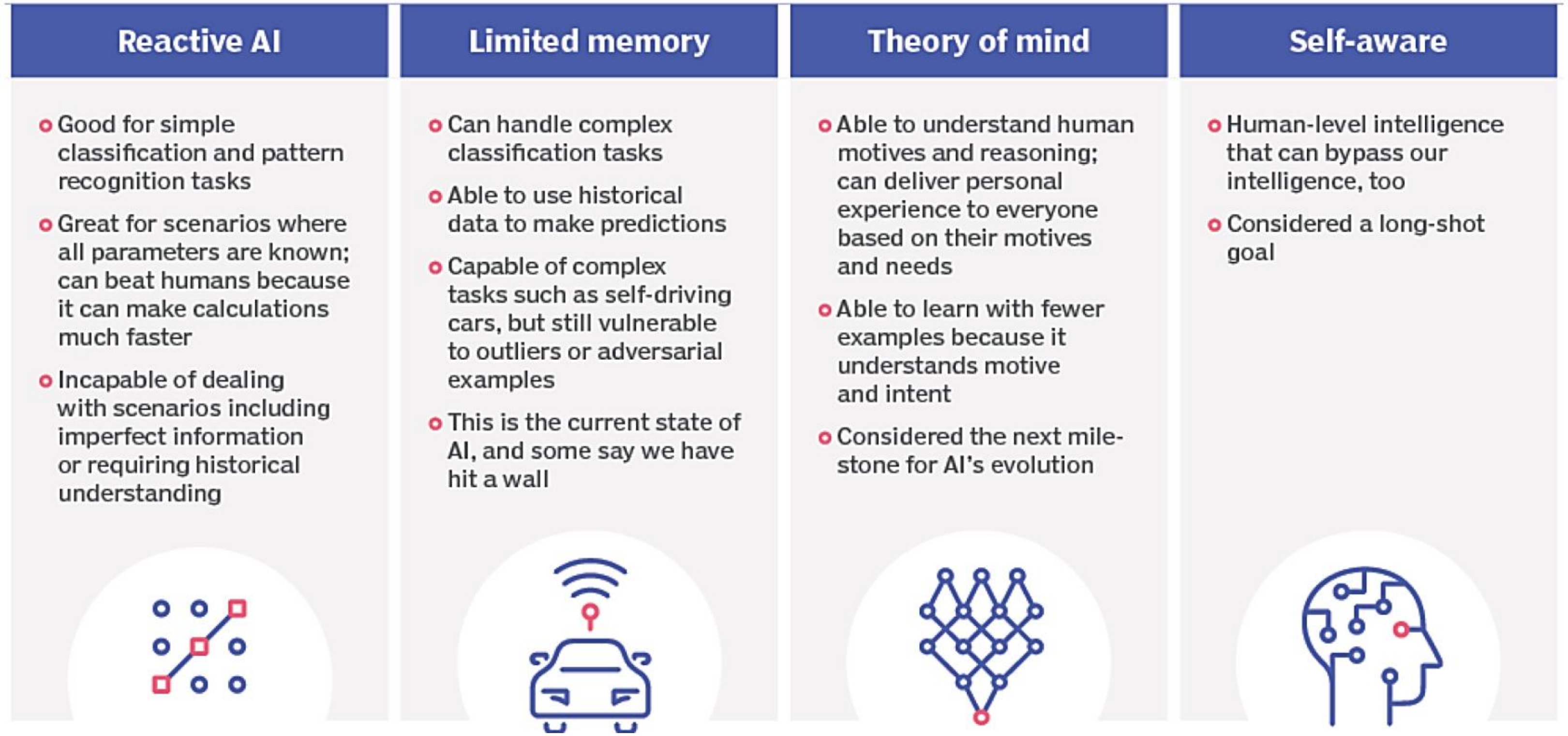
AI Capabilities

Artificial Narrow Intelligence (ANI): Performing narrowly defined sets of tasks

Artificial General Intelligence (AGI): Simulating thought processes of the human mind

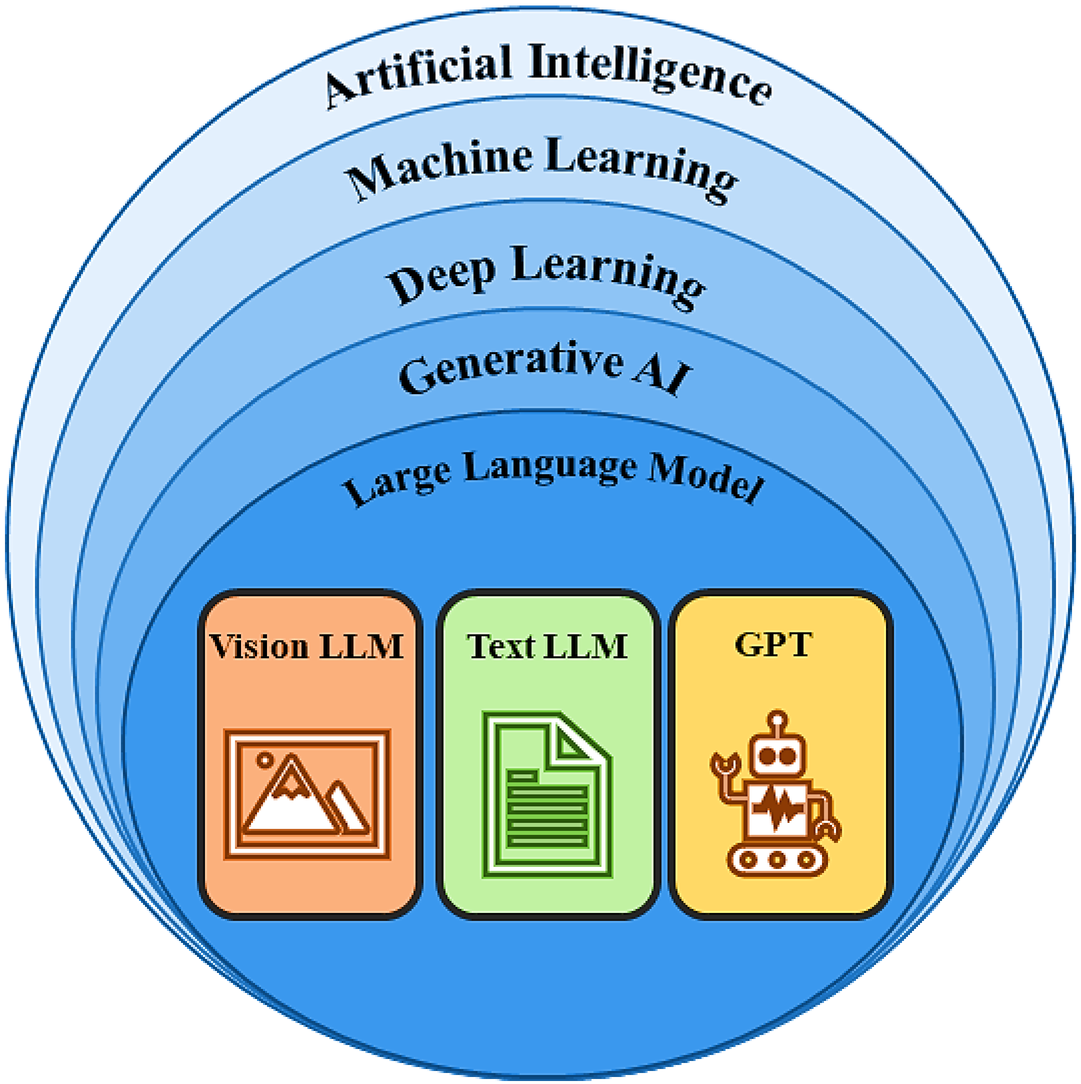
Artificial Super Intelligence (ASI): Performing beyond human capability

AI Systems[1]



1: Prof. Arend Hintze's (Dalarna University, Sweden) Hypothesis

Sub-fields of AI

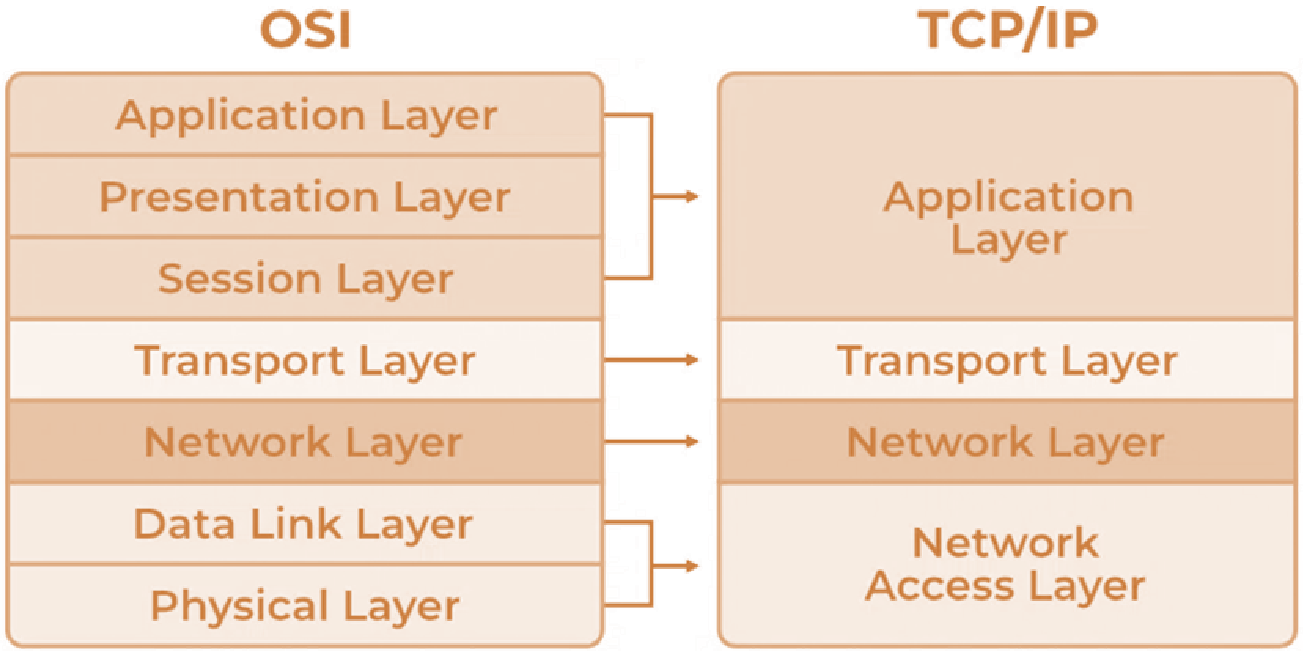


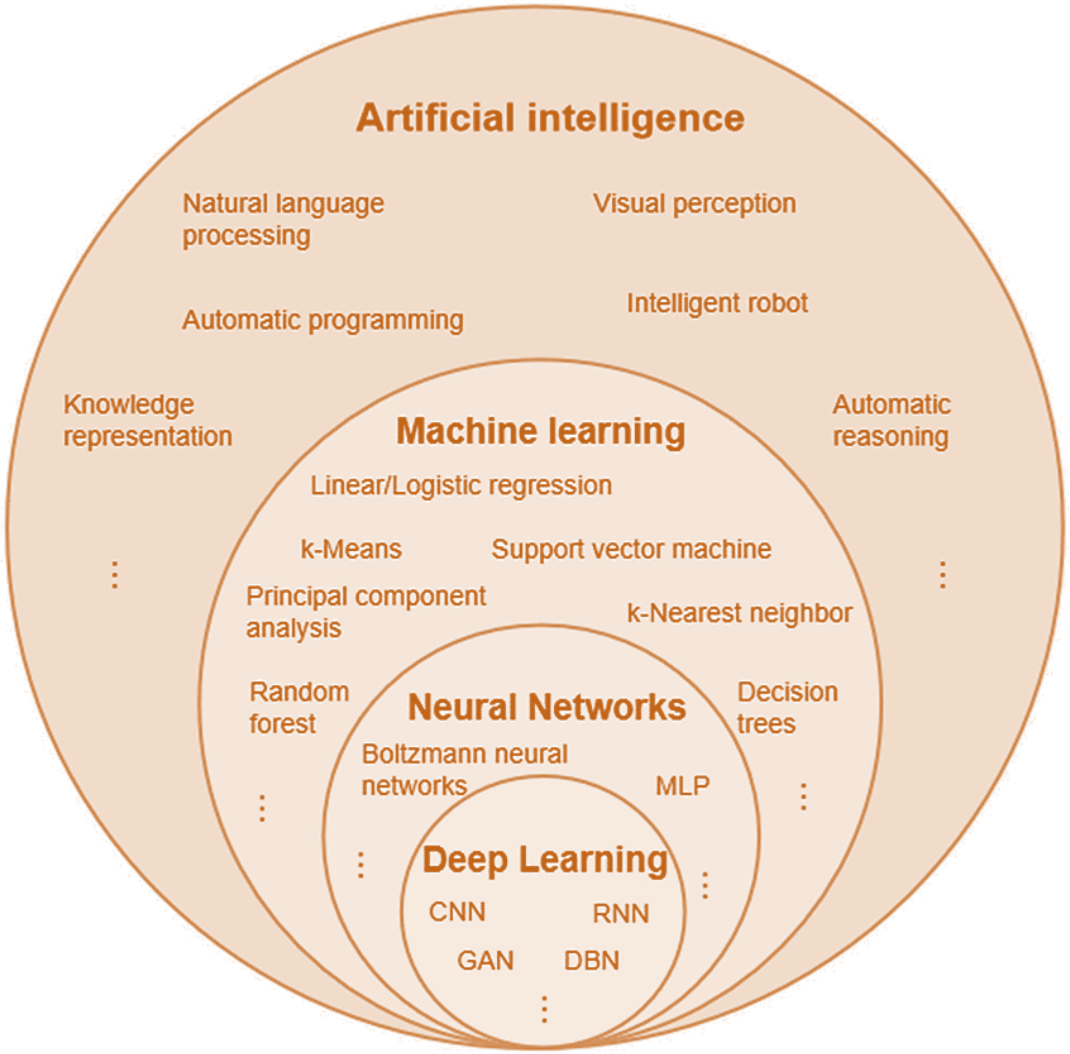
Core Areas - Artificial General Intelligence

AI/GAI

- AL, DL, ANN
- Computer Vision
- Robotics, Intelligent Agents
- NLP
- TTS and STT
- Expert Systems, Knowledge Representation and Reasoning
- Autonomous Vehicles
- Augmented and Virtual Reality
- Social Networks and Graph Analysis

AI Layer Hierarchy





Real-world Applications of AI

Healthcare	CRM	Finance	Manufacturing	Transportation
• ML algorithms are facilitating early disease detection, accurate diagnosis, personalized medicine etc.	• NLP powered virtual assistants, chatbots providing 24*7 uninterrupted human-free service • ML algorithms to identify buyers' behaviour, preferences to provide **hyper-personalized customer experience** • Algorithms can automatically generate customized product recommendations, promotions and content for customers and prospects	• ML algorithms are employed for fraud detection, algo trading, credit scoring and risk assessment • AI-powered financial planning and wealth management platforms, robo-advisors leverage advanced algos to analyze markets trends, assess client risk tolerance, provide personalized investment recommendations	• Advanced algos to detect defects in products to ensure quality, predictive maintenance, supply chain optimization, robotics	• Self-driving cars, route optimization, public transport passenger demand prediction, schedules optimization etc.

Real-world Applications of AI

Agriculture

- Precision farming with AI farmers - data-driven decisions for irrigation optimization, improved fertilization and reduced waste.
- AI to monitor crops for infestation and appropriate pesticides, identify predict yields etc.
- Self-driven tractors for farming, drone-driven pesticide sprinkling and spraying etc.

Retail

- Personalized shopping experience, personalized product recommendations, just-in-time inventory,

Education

- AI-driven language translation, real-time transcription and sub-titles
- Automatic grading of answers/solution

Energy

- Smart grid management, demand forecasting, predict usage patterns for efficient handling of power generation/sourcing etc.

Human Resources

- Automatic resume screening, advanced algos for creating, assessing job posts etc.

Business Intelligence

- Insights and recommendations generated by AI models can help take data-driven decision-making for businesses efficiency and growth

Real-world Applications of AI

Government

- AI is being used to improve public safety, detect crime, and provide citizen services

Security

- AI algos for facial recognition, surveillance, and threat detection

Entertainment

- AI-generated content for immersive experience – VR, AR
- AI-powered recommendation and content curation for engaging and personalized entertainment experience

Law and Legal

- Identifying potential issues in contracts, legal documents, and expediting legal research by extracting relevant information using AI-driven tools

Space

- AI is employed for space craft navigation, satellite imaging, mission planning, new astronomical phenomena identification etc.

How Do Machines Learn?

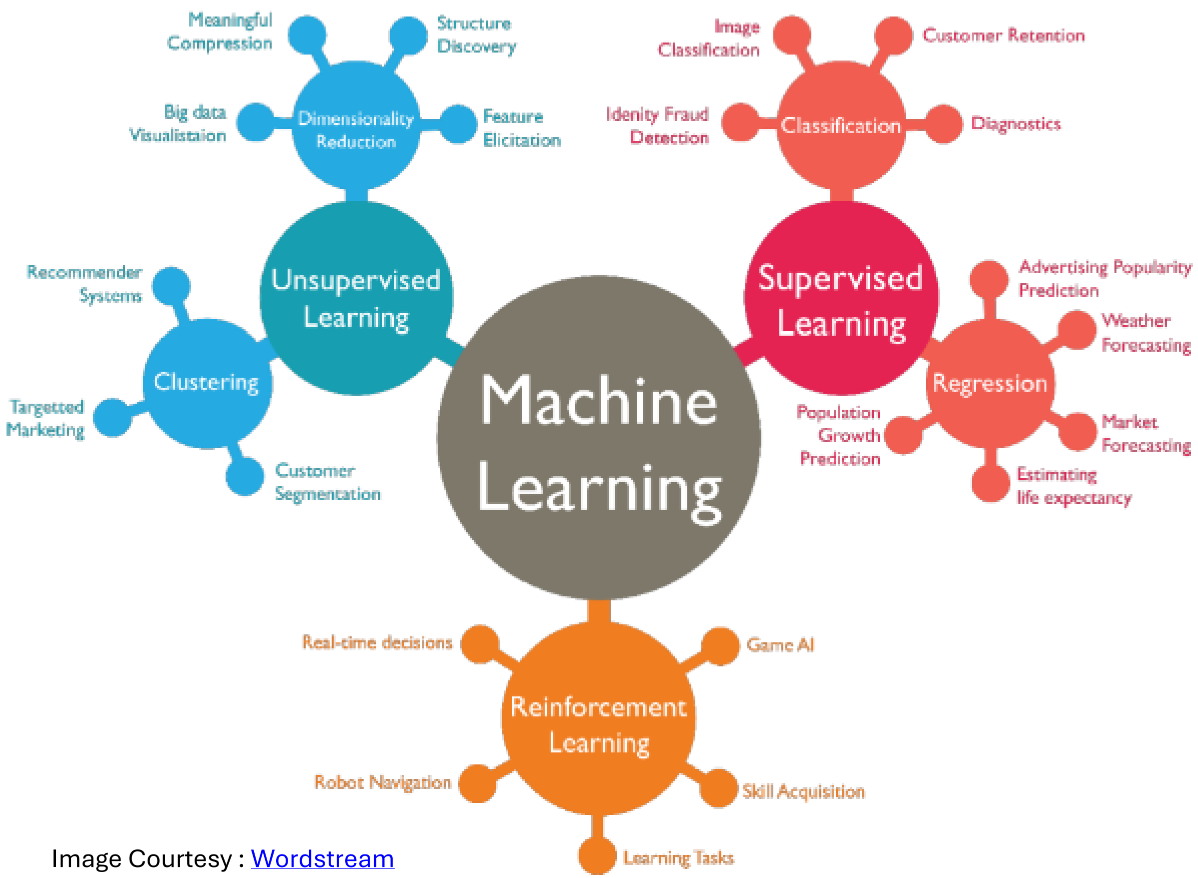


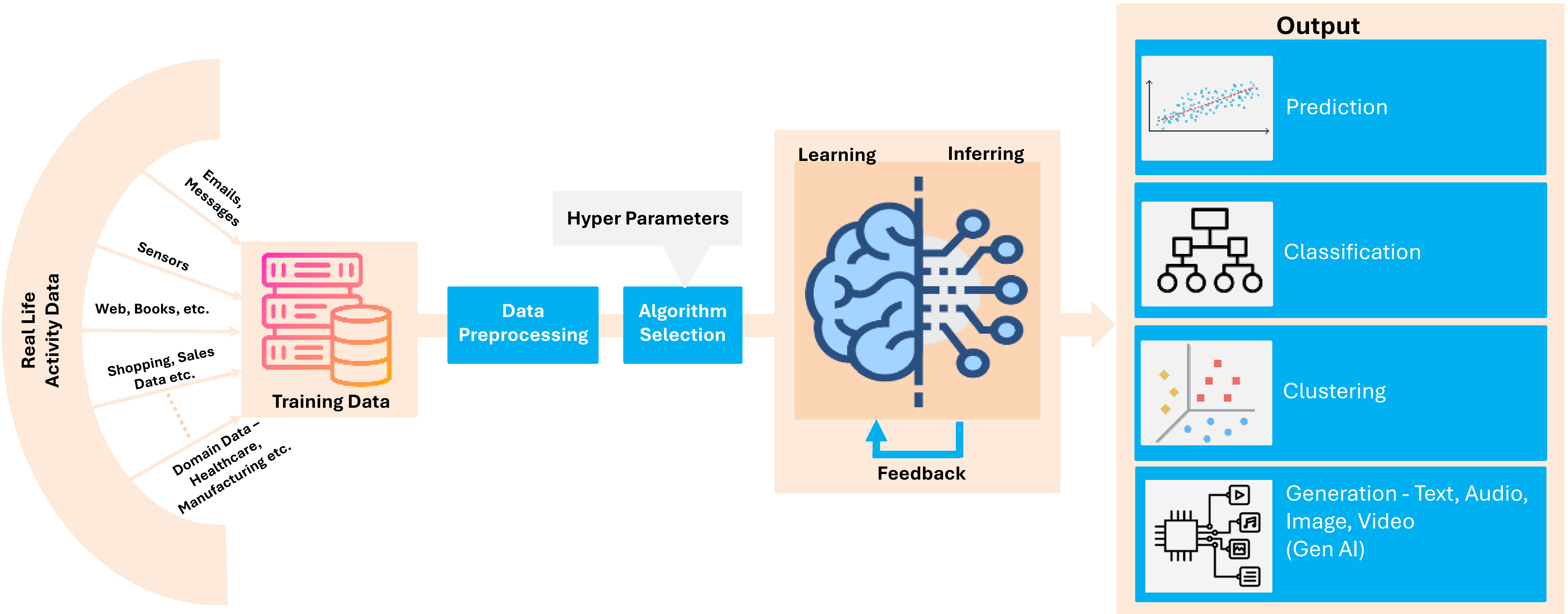
Image Courtesy : [Wordstream]

- Can a computer learn without explicit instructions?
- How do AI models make sense of the vast amounts of data they are fed?
- What makes a machine get better over time?

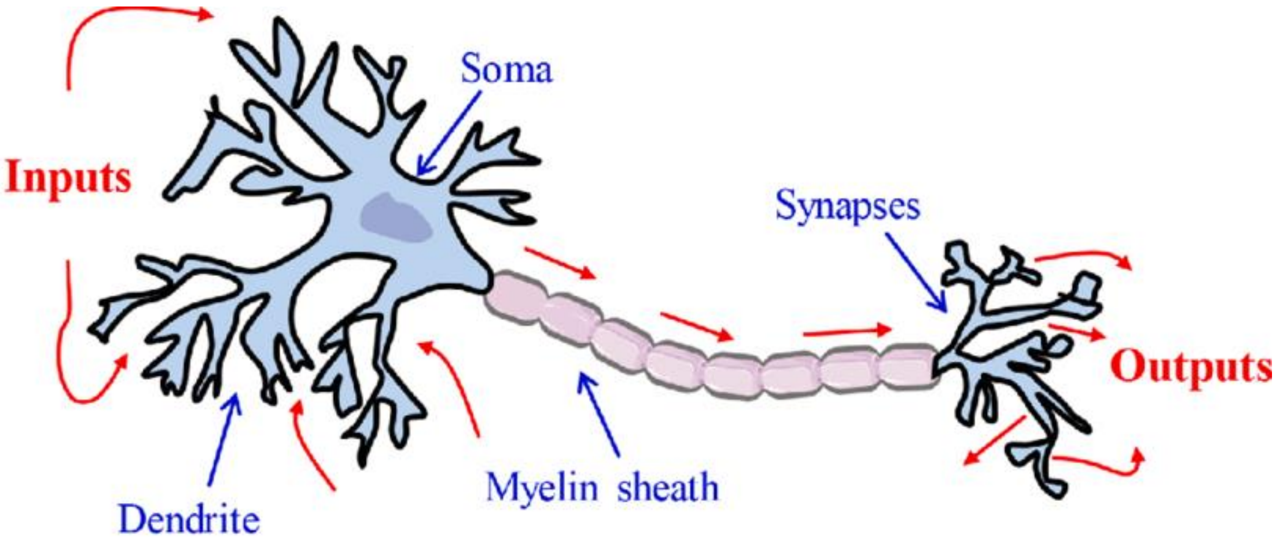
We don't need to teach a machine to think like us; we need to teach it to learn from us

- Yann LeCun, Deep Learning Pioneer, Chief AI Scientist at Meta and Professor at New York University

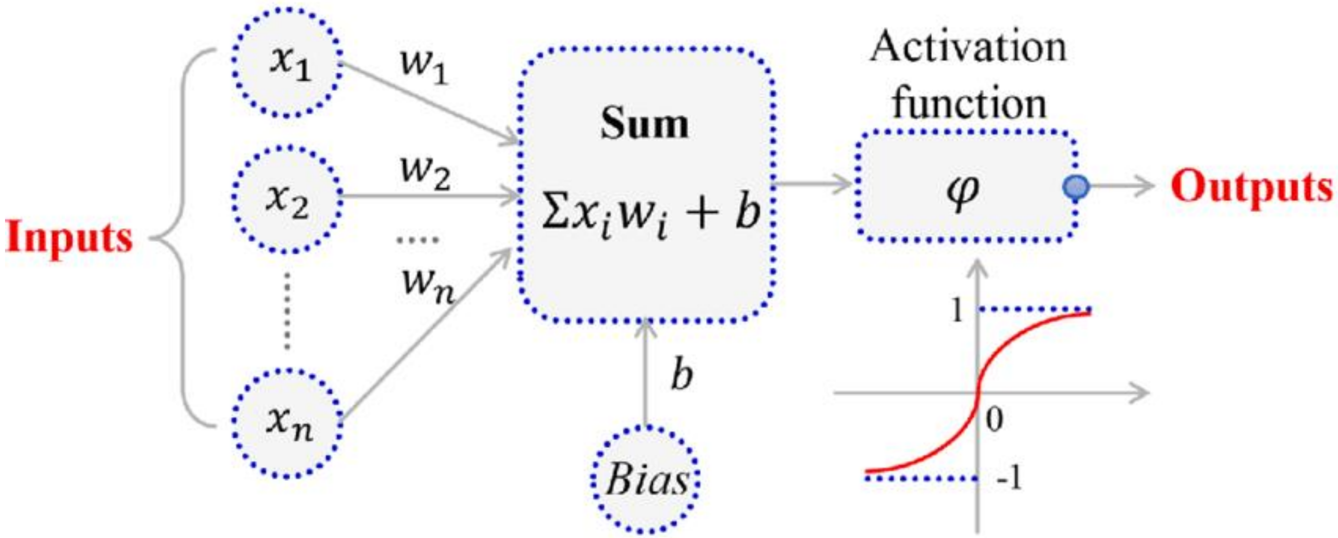
How Do Machines Learn? (Contd..)



AI Key Concepts - Biological and Mathematical Neurons

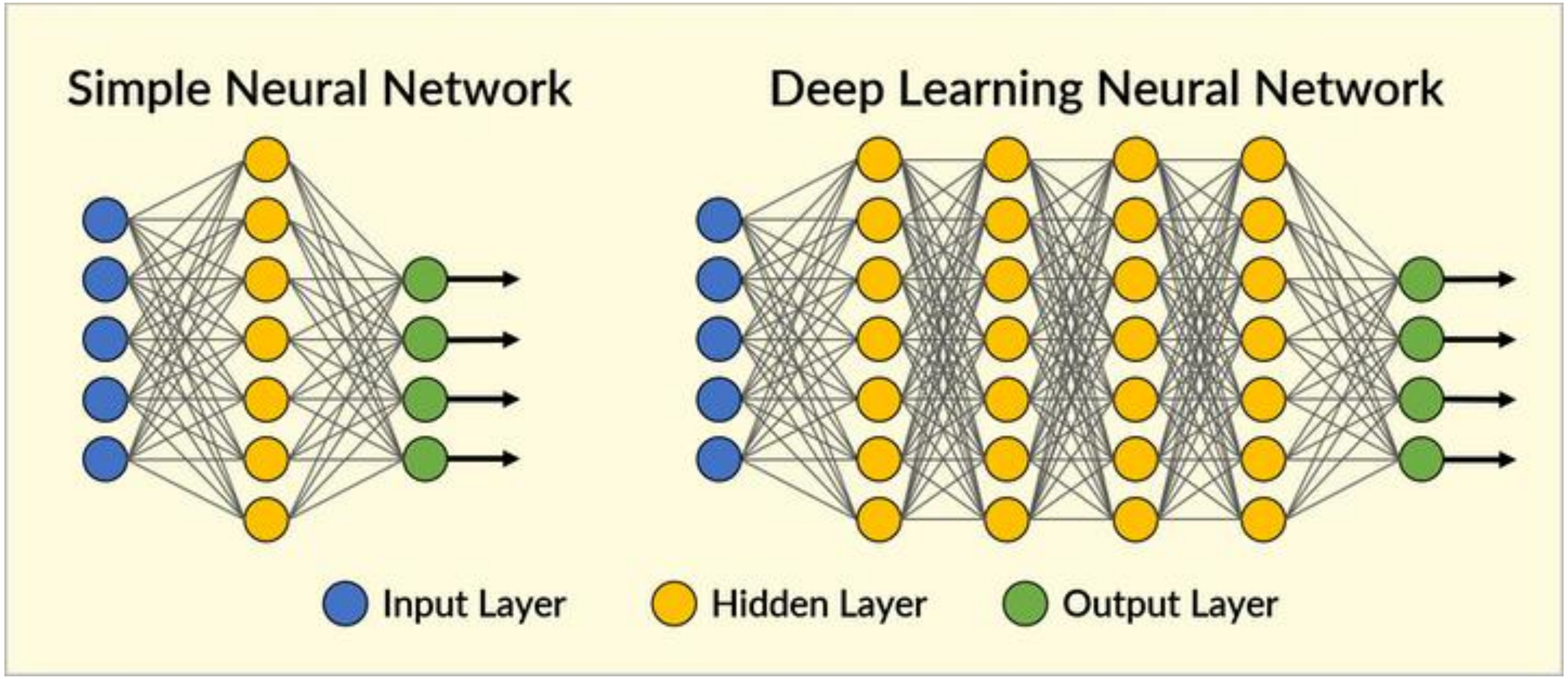


(a) Biological neuron

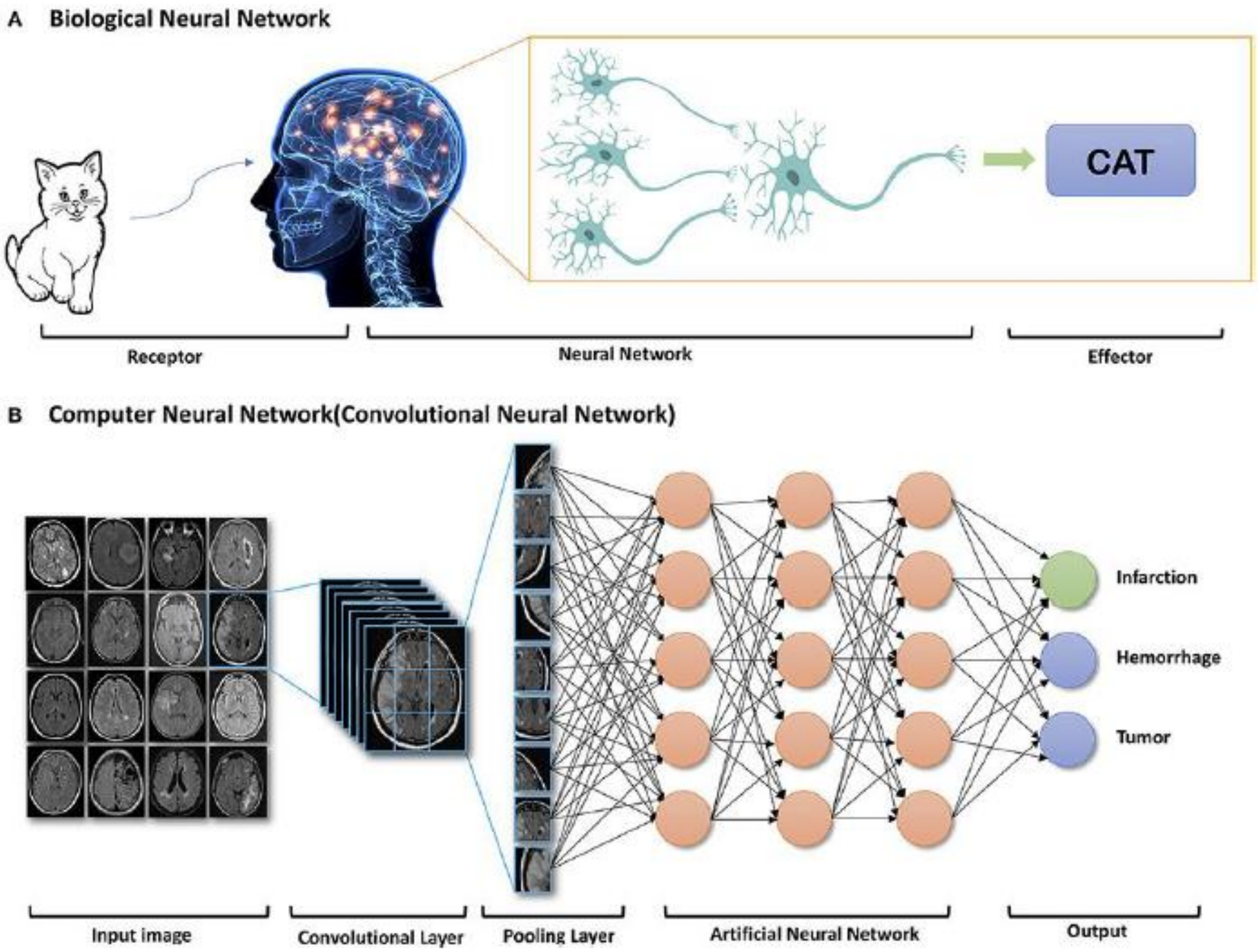


(b) Artificial neuron

AI Key Concepts - Deep Learning

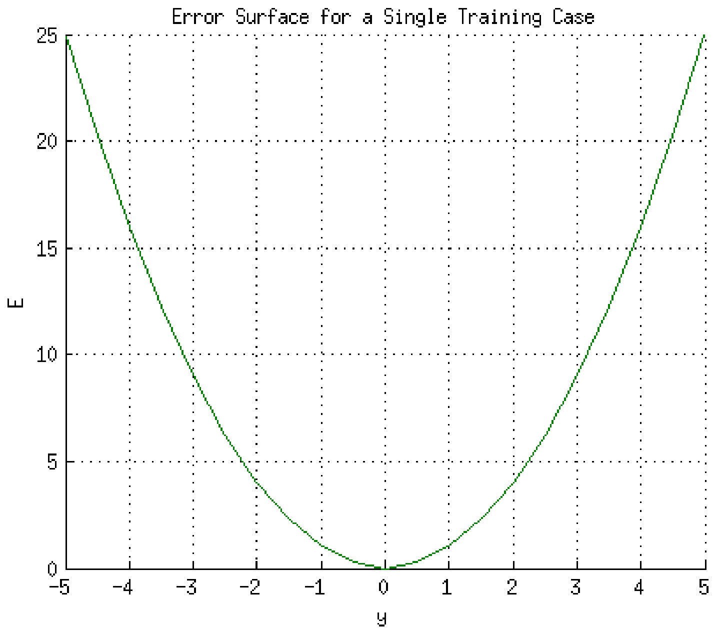


AI Key Concepts - Deep Learning

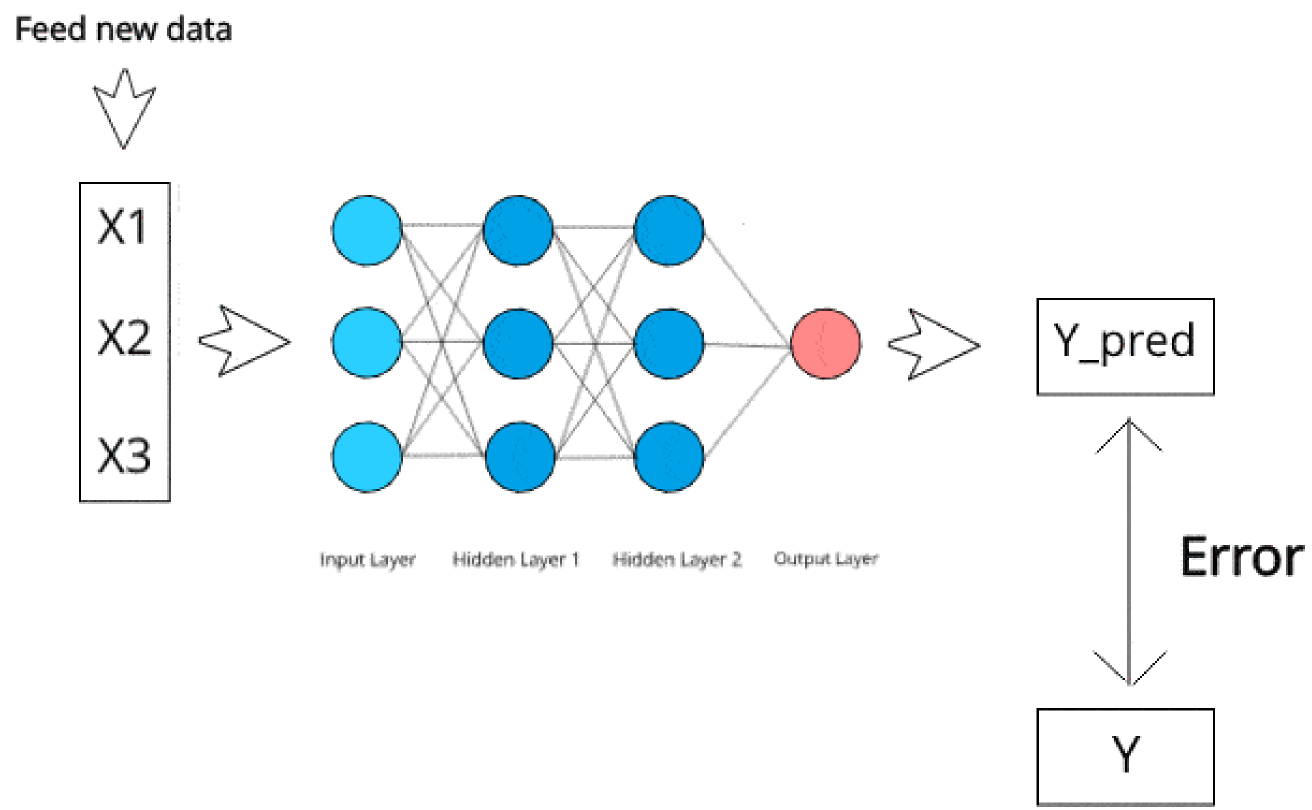


AI Key Concepts - Back-propagating Error Correction aka Backpropagation

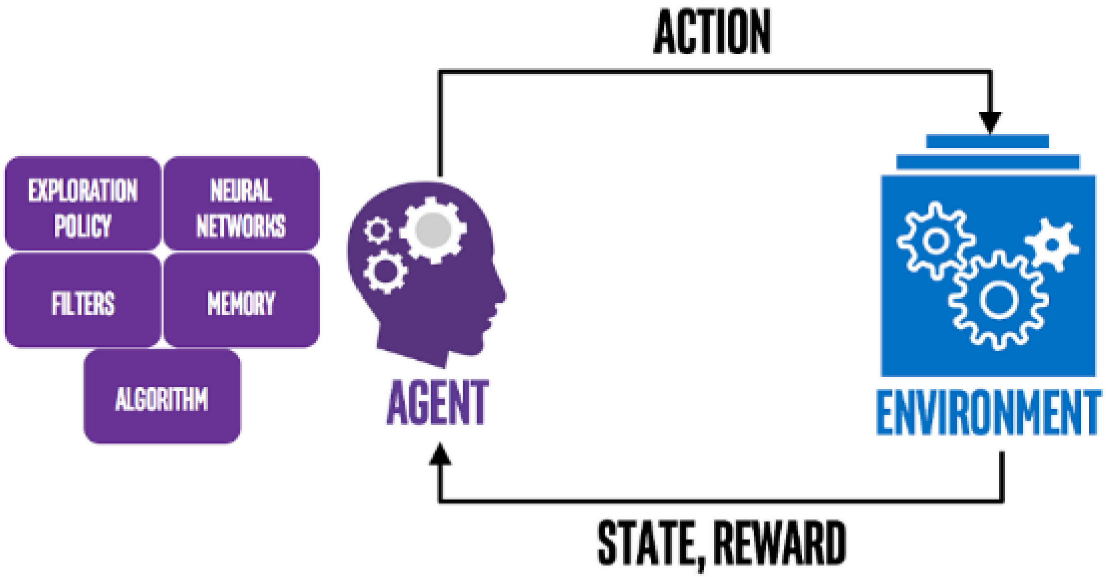
- Goal of any supervised learning algorithm (ML or DL) is to find a function that best maps or fits set of inputs (x_1, x_2) to their outputs (t)
- Initially, with random weights, the predicted output y which is likely to differ from $t - y = w_1 * x_1 + w_2 * x_2$
- Consider one-shot training case with tuple (1,1,0)
- The loss or cost function $\mathcal{L}(t, y) = E = (t - y)^2$ - Squared Error
- The minimum of **"E vs y plot"** corresponds to output y which minimizes the error E (to 0)
- Finding **the mapping or learning function** boils down to an **optimisation problem** of **finding a function that will produce minimal error**
  - $\boldsymbol{f() = \min_{s.t. y = (w_1 * x_1 + w_2 * x_2)} \mathcal{L}(t, y)}$
- Backpropagation is a gradient estimation method during training neural networks to compute the network parameter updates
- It is a chain rule that computes the gradient of the loss function with respect to weights of the network for single input-output - one layer at a time iterating backward from the last layer
- Backpropagation refers only to an algorithm for efficiently computing the gradient, not how the gradient is used



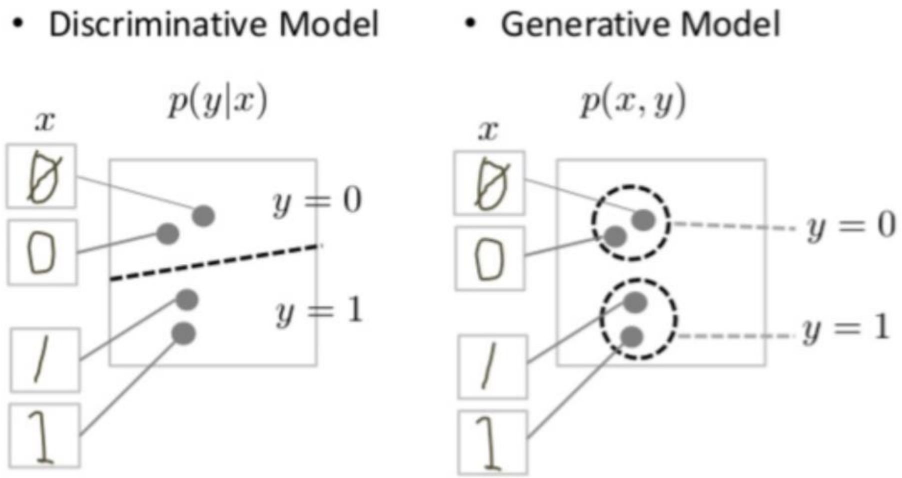
AI Key Concepts - Back-propagating Error Correction aka Backpropagation (Contd...)



AI Key Concepts - Reinforcement Learning



AI Key Concepts - Generative Vs Discriminative Models



Aspect	Discriminative Models	Generative Models
Objective	Model the conditional probability (P(Y | X)	Model the joint probability P(X,Y)
Focus	Learn the boundary that separates different classes	Understand the underlying distribution of data
Examples	Logistic Regression, SVM, Neural Networks, Random Forests	Naive Bayes, Gaussian Mixture Models, HMM, VAEs
Advantages	Better classification performance, directly optimizes decision boundaries	Can generate new data, handles missing data well
Disadvantages	Cannot generate new data, requires a lot of labeled data	Requires assumptions about data distribution, less accurate for classification tasks
Usage	Classification, regression	Data generation, density estimation

AI Timeline

Artificial Intelligence

Engineering intelligent machines and programs

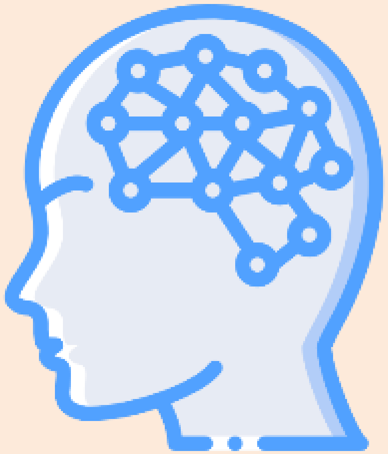
1950 – 1970

Machine Learning

Making computers learn without being explicitly programmed

1980 - 2006

Deep Learning



Learning based on Deep Neural Networks and vast amounts of data

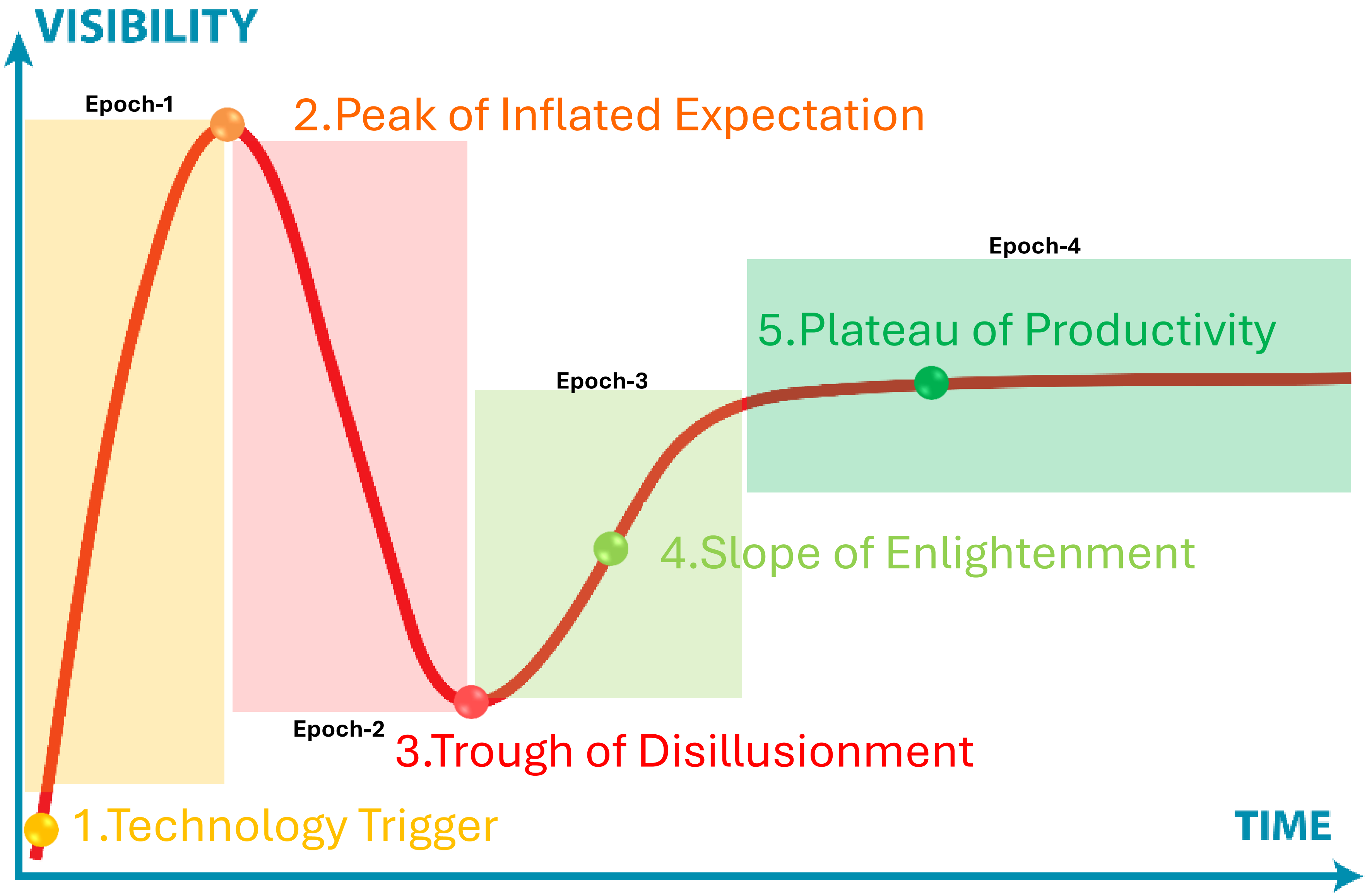
2010 - 2017

GPTs and LLMs

Building large foundational pre-trained language models to recognize, translate, predict, or generate text or other content

2018 - 2024

New Technology Journey in Business



Created and popularized by Gartner as **Gartner Hype Cycle**

Key Enablers for AI's Growth in 21st Century

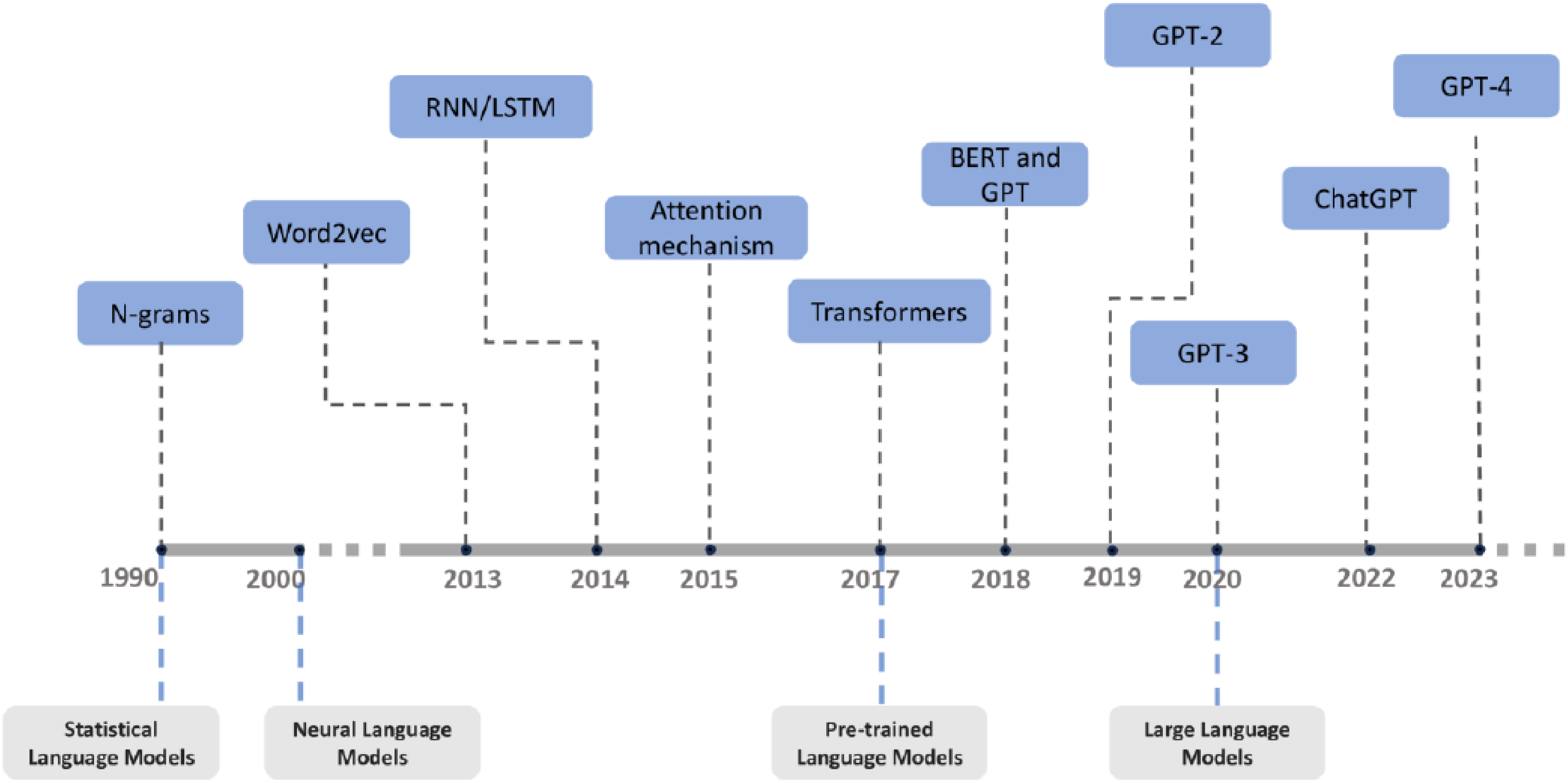
Advances in computing power – GPU, TPU, AI Chips

Cloud, User Generated Content, Vast Amounts of Web Data and Digital Assets

Continuous Improvements in AI

Advances in NLP – Transformer, GPTs, LLMs

NLP, GPT and LLMs Timeline



GPTs and LLMs

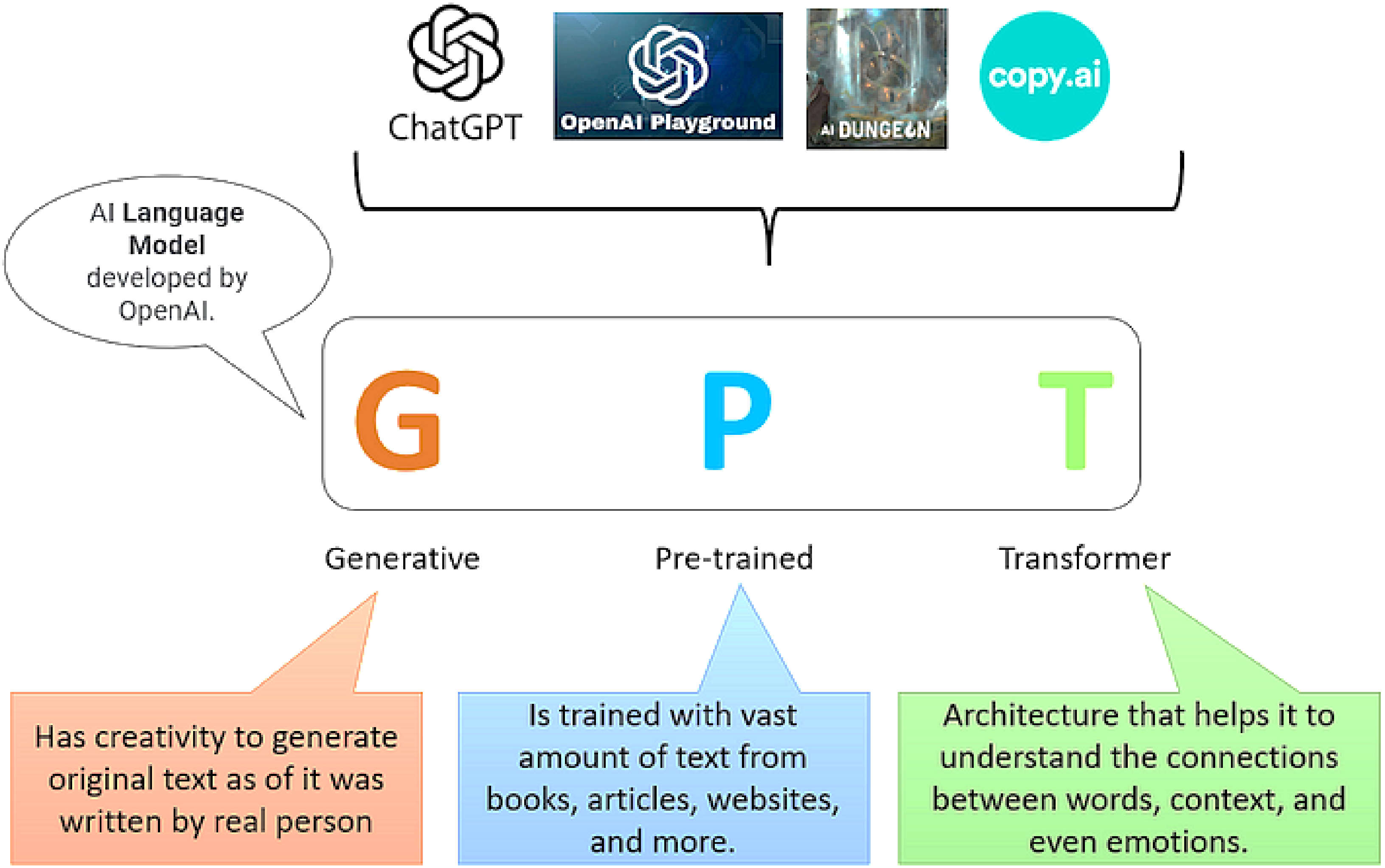
GPTs – Generative Pre-trained Transformers

- Specific type of LLM developed by OpenAI is designed specifically for generating coherent and contextually relevant text.
- Example : GPT-1, GPT-2, GPT-3, and GPT-4 of OpenAI
- Generates human-like text given some input or prompt.
- Pre-trained on Peta bytes of text in an unsupervised manner and fine-tuned
- Unidirectional: Traditional GPT models are autoregressive, meaning they generate text one token at a time, considering previous tokens

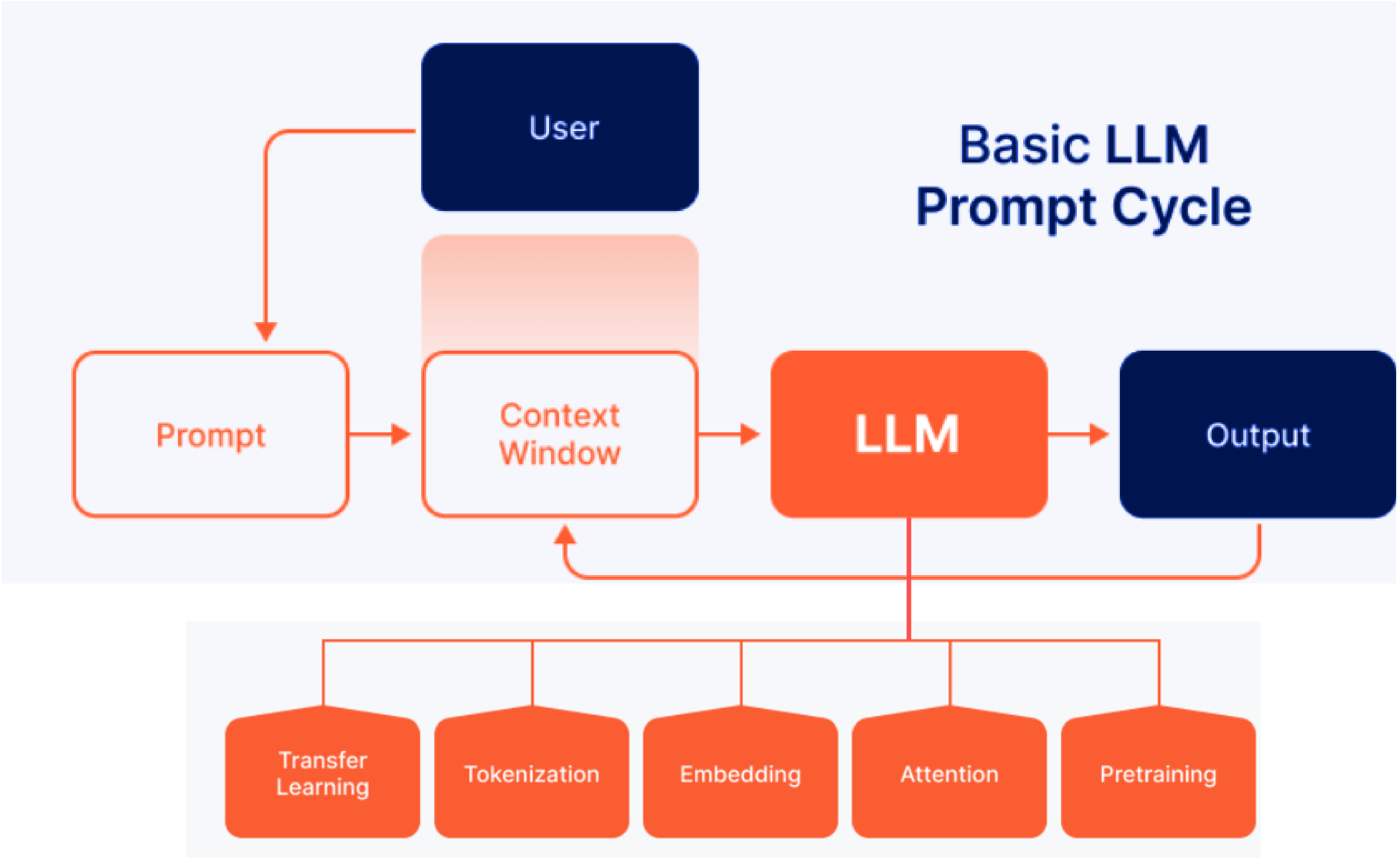
LLMs – Large Language Models

- Language model trained on a large corpus of text data designed to understand, generate, and manipulate human language
- Examples: GPT (all versions), BERT, T5, LLaMA, and PaLM
- Have large number of parameters - ranging from millions to hundreds of billions
- **Trained on** vast amounts of text data from the internet, books, articles, etc.
- **Perform variety of NLP tasks -** text generation, translation, summarization, sentiment analysis, question answering, and more.

GPT


ChatGPT
OpenAI Playground
AI DUNGEON
copy.ai
AI Language Model developed by OpenAI.
G
P
T
Generative
Pre-trained
Transformer
Has creativity to generate original text as of it was written by real person
Is trained with vast amount of text from books, articles, websites, and more.
Architecture that helps it to understand the connections between words, context, and even emotions.

LLM Functional Architecture

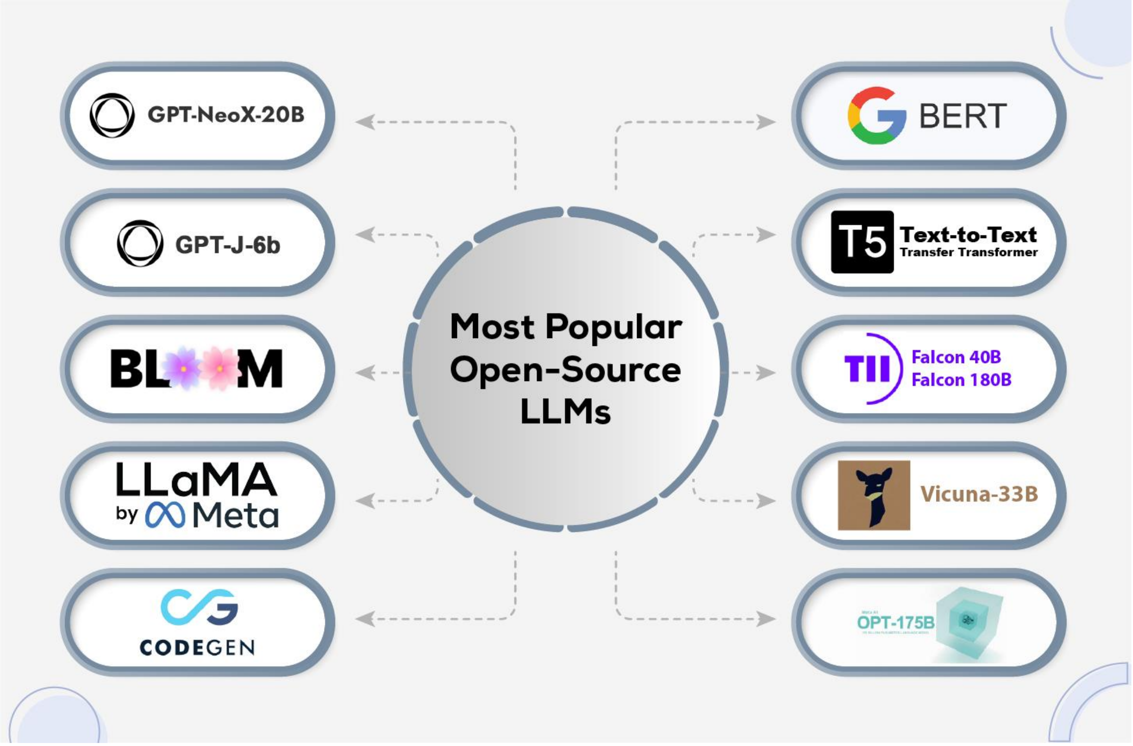


LLM Compute Requirements

Model	Parameters	Training Data	Training	Inference
BERT	340 million	3.3 million words	6.73^10^18 FLOPS	680 GFLOPS
GPT-J	6 billion	402 billion tokens	1.45*10^22 FLOPS	12 TFLOPS
GPT-3	175 billion	300 billion tokens	3.14*10^23 FLOPS	350 TFLOPS

Computational effort required for training (all training data) and inference (1024 tokens) for a number of popular text models.

LLMs – Closed and Open Source



Closed Source LLMs

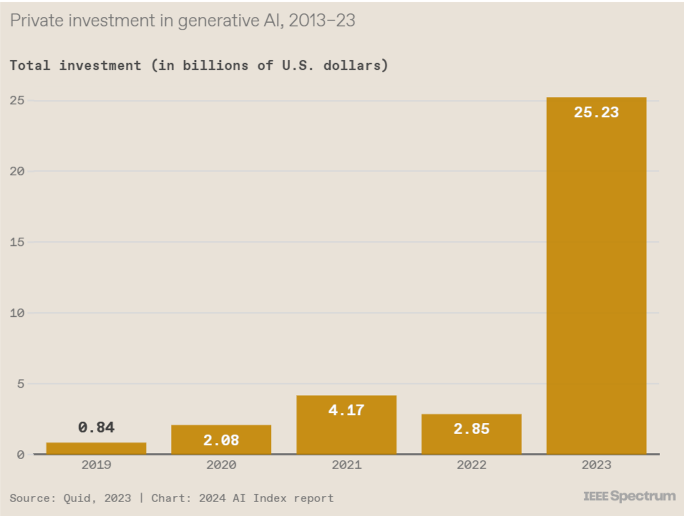
- GPT-3 and GPT-4
- Megatron Turing NLG
- ERNIE 3.0
- Titan
- Jurassic-1
- Wu Dao 2.0
- HyperCLOVA
- Gopher
- Chinchilla
- Galactica
- LaMDA
- AlexaTM
- BloombergGPT
- PanGu
- Kosmos-1
- Sarvam's OpenHathi-Hi-v0.1
- Ola's Krutrim LLM
- BharatGPT

GPT-3 – Training Corpus

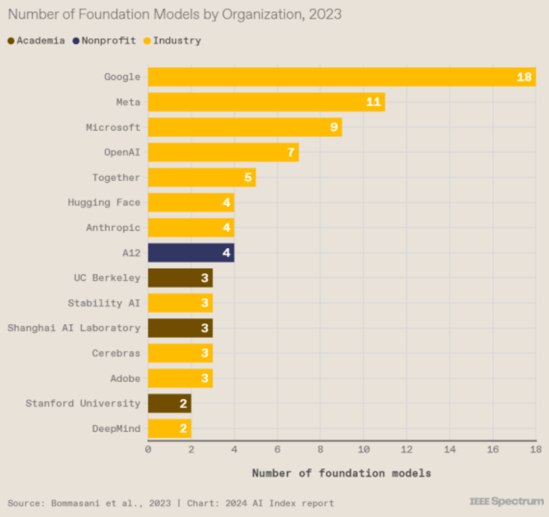
- Common Crawl Data
- Books
- Wikipedia
- Research Papers
- Curated Web Sources
- Code Repositories
- Dialogue Datasets
- News Articles

Datasets	Quantity (Tokens)	Weight in Training Mix	Epochs elapsed when training for 300 BN tokens
Common Crawl (filtered)	410 BN	60%	0.44
WebText2	19 BN	22%	2.90
Books1	12 BN	8%	1.90
Books2	55 BN	8%	0.43
Wikipedia	3 BN	3%	3.40

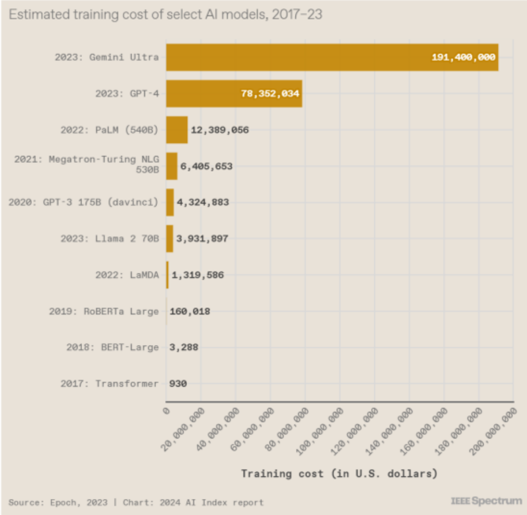
AI State of the Art - 2024



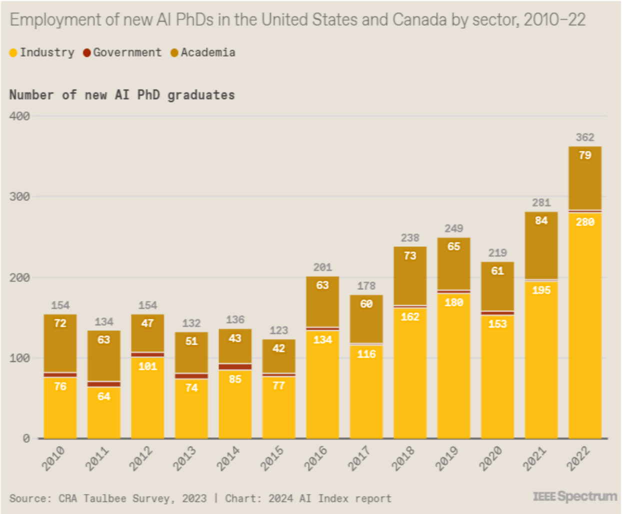
Generative AI investment skyrockets



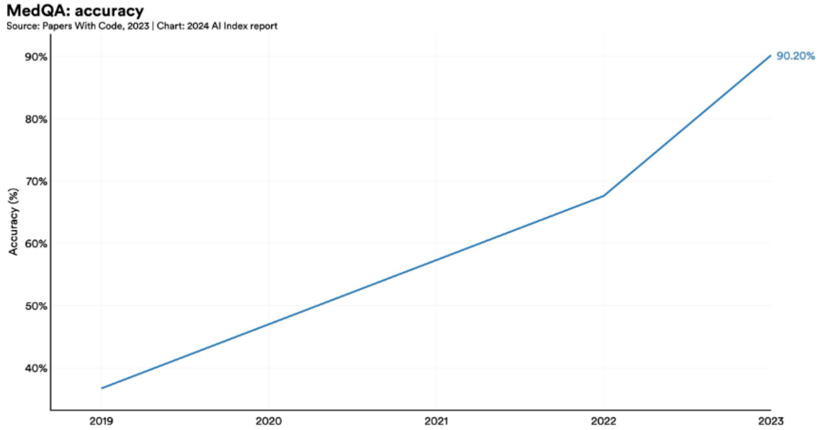
Google is dominating the foundation model race



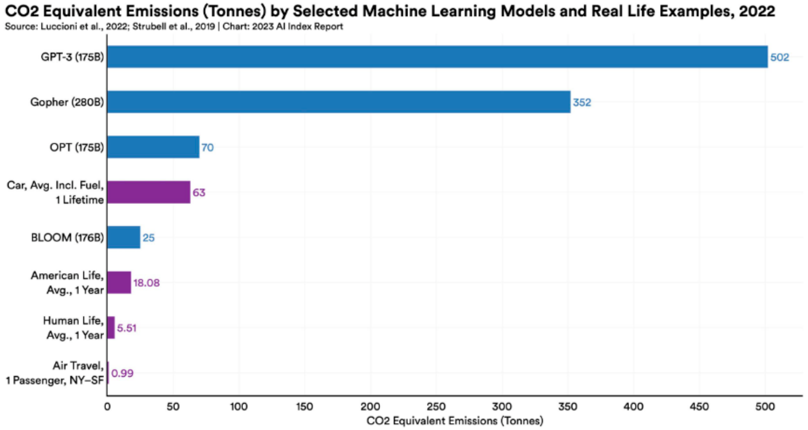
Foundational models have gotten super expensive



Industry calls new PhDs



GPT-4 Medprompt, a stand-out model of GPR-4 has reached an accuracy rate of 90.2% in clinical knowledge

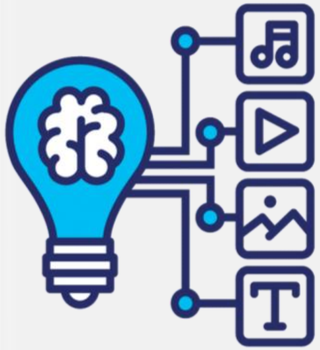


AI systems can have serious environmental impacts!

[Source: Stanford's 2024 AI Index Tracks Generative AI and More - IEEE Spectrum]

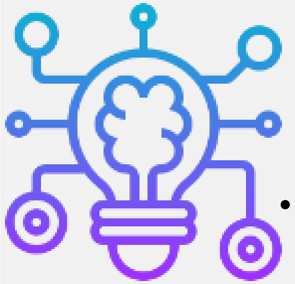
State of the Art in AI

Generative AI



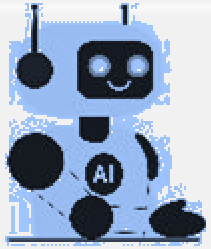
- **LLMs:** OpenAI's GPT-4, Google's PaLM, Meta's LLaMA, and Anthropic's Claude are being integrated into various applications such as chatbots, content creation, coding assistance, and more.
- **Multimodal Models:** OpenAI's GPT-4 Vision and DeepMind's Gemini combine language, vision, and other modalities can analyze images, generate descriptions, and even perform image editing.
- **Diffusion Models: D**iffusion models like DALL-E 3, Midjourney, and Stable Diffusion have set new standards for generating high-quality, realistic image, video, and audio content

RL



- **Real-World Applications:** RL is being applied to robotics like iRobot's Roomba vacuum cleaner, autonomous driving, supply chain optimization, and personalized recommendations, where agents learn optimal strategies by interacting with their environments.
- **Advancements in Game AI**: RL models like AlphaZero and MuZero have demonstrated the ability to learn complex strategies in games such as chess, Go, and even real-time strategy games without human data.

XAI



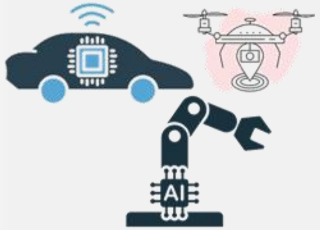
- IBM's AI Explainability 360, DARPA's XAI program, SHAP (SHapley Additive exPlanations) models and frameworks help understand and interpret the decision-making processes of AI systems, essential for ensuring transparency, accountability, and trust, especially in critical domains like finance and healthcare.

State of the Art in AI

AI in Healthcare

- IBM Watson for Oncology, Google's DeepMind AI for protein folding (AlphaFold), PathAI for pathology are revolutionizing healthcare by improving diagnostics, drug discovery, personalized treatment plans, and monitoring patient health.

AI in Autonomous Systems



- Tesla's Full Self-Driving (FSD) mode, Waymo's autonomous taxis, Boston Dynamics' AI-driven robots etc. are advancing self-driving cars, drones, and robots, enabling them to perform tasks autonomously in dynamic and complex environments.

AI for Sustainability

- Google's AI for predicting flood patterns, Climate AI for crop yield prediction, DeepMind's energy-efficient cooling for data centers address environmental challenges, including climate change mitigation, optimizing energy consumption, and predicting natural disasters

Dangers of AI

- Automation Spurred Job Losses/ Displacements
- Deepfakes
- Privacy Violations
- Social Manipulations Through AI Algorithms
- Algorithmic Bias Caused By Bad Data
- Market Volatility
- Autonomous Weapons Powered by AI
- Un-controllable Self-aware/ Sentient AI

Challenges and Limitations

- Lack of transparency
- Bias and Discrimination
- Privacy Concerns
- Ethical Dilemma
- Mis-use/ Security Risks
- Concentration of Power
- Potential Job Displacement
- Dependence on AI
- Economic Inequality
- Legal and Regulatory Challenges
- Loss of Human Connection
- Existential Risks (AGI)

Future Direction of AI

Generalized and Multimodal AI Systems

- Beyond Narrow AI : Generalized Multi-modal AI models (text, image, audio, video etc.) across different domains with an underlying unified architecture
- Unified AI Models : Integration of different AI paradigms – supervised, unsupervised, reinforcement learning etc. – into a single, versatile model that can learn from diverse types of data and feedback reflecting more human-like learning capabilities

Efficient and Scalable AI

- Model Efficiency and Optimization : Reduction in compute footprint, energy consumption etc.
- Federated and Edge AI : Models are trained on devices than on centralised servers, enhancing privacy, reducing latency, and enabling real-time decision-making

Explainable and Interpretable AI – XAI

- Trust Worthy AI Systems - Bringing transparency and understandability of AI systems to humans through explainability and interpretability of their internal decision making process
- Causality in AI – Incorporating causal reasoning into AI model to go beyond correlation-based learning to usher in decision making based on deeper understanding of cause-and-effect relationship

Ethics, Fairness and Responsibility

- Bias mitigation and fairness techniques to mitigate bias and enhance fairness in AI models to ensure they do not perpetuate or amplify societal inequalities

Future Direction of AI

Domain Specific AI Applications

- Specially fine tuned and trained models for different domains – healthcare, finance, education, manufacturing, legal, climate sciences etc.

AI for Social Good and Human-AI Collaboration

- AI tools to address global challenges like climate change, food security, public health, disaster management etc.
- Creating AI tools that enhance the creativity, productivity, and decision-making in the fields of art, design, engineering, customer service etc.

AI Governance and Regulation

- Establishing global standards and regulatory frameworks to govern the development and deployment of AI technologies

Next generation AI Architectures

- Exploration of new computing paradigms - To overcome the limitations of classical computing enabling faster and more efficient processing of vast data sets - Neuromorphic Computing, Quantum AI etc.
- Self-supervised and Few-Shot Learning – Learning from unlabelled data and from few examples making AI learning process more data-efficient and adaptable to new tasks with minimal retraining

“GAI would be a pervasive and ubiquitous API utility in each technology solution on the planet like a RESTful End-point”

AAM-IPL Overview

Program benefits

- Hands-on experience in coding and implementing AI/ML algorithms using real-world industry data
- Lab will guide students through the practical application of key ML techniques
- Students will engage in project-based learning, applying AI and ML techniques they have learnt in their curriculum to address practical industry challenges
- Bridge the gap between theoretical knowledge and practical application of ML algorithms
- Invaluable insights into current industry practices and trends
- Enhancing technical proficiency for successful careers

ML algorithms addressed

- PCA, Linear Regression, Logistic Regression
- Support Vector Machines, K-means clustering, Naive Bayes
- Multi-variate Gaussian Discriminant Analysis, Decision Tree Classification

Pre-requisites

- Completion/studying ML course of CSE(AIML) scheme 2020
- Students are expected to be familiar with basic concepts of
  - Linear Algebra, Properties and Matrices operations
  - Calculus – differential, integration
  - Convex Optimization etc.

AAM-IPL Overview

Structure of the Course

- Each Monday 8:00 PM IST
- Next Project Announcement – Topic, Data Set, Shell Code
- Announcement Channels – Google Classroom, Industry Projects WhatsApp Group
- Each Saturday 10:30 AM IST – 12:00 Noon IST
- Overview of the algorithm and project, interactive Q&A on the project implementation
- Each Sunday 10:30 AM IST – 12:00 Noon IST
- Project implementation, output demonstration, interactive Q&A
- Each Sunday 11:59 PM IST
- Deadline to submit/upload completed week's project code onto Google classroom
- All online classes will be through Google Meet (provided by Brillium Technologies)
- Project submissions will be graded

Tools and Technologies

- Computing Language – Python
- IDE – Visual Studio Code with Jupyter Notebook
- Online Data Sets for Training - Datacamp, Kaggle, Wikipedia

Online Google Classroom

- FCH, presentation slides, projects data, problem statement will be uploaded to AAM – IPL Google Classroom ahead of the respective sessions
- Program schedule is available in Google Classroom

Program and Lab Coordinator

- Prof. V. Suresh - vsuresh.ecs@gprec.ac.in

Interested in Gen AI Projects?

- Reach out to venkat@brillium.in with your idea

Q&A

Call To Action

- Asking questions – there is **No Stupid Question**
- Understanding **the algorithm** of the project **early in the week after announcement**
- Asking project implementation related **questions on each Saturday/project overview sessions**
- Implementing the project **before each Sunday session** and demonstrating the output, if asked
- Seeking help to completing the project **in Sunday sessions** ,if needed
- Submitting the completed project code (runnable) **by each 11:59 PM IST on Sunday**

Interested in building a Gen AI application?

Reach out to venkat@brillium.in

THANK YOU!

AAML-IPL Brought You in Partnership with:

Brillium Technologies

Sector 7, HSR Layout, Bengaluru 560102, Karnataka, India
Website: www.brillium.in | Email: connect@brillium.in