

A large, diverse group of people of various ages and ethnicities are seated in a classroom, looking towards the front. The scene is brightly lit with large windows in the background. A semi-transparent dark box with a thin white border is positioned in the upper right, containing the title text.

Demystifying AI

Prof. Kevin D. Jones



Our Objective:

Provide a foundational understanding of what AI is and how it works in simple terms. This class should empower attendees with the knowledge to understand AI and several useful AI tools.



Learning Outcomes:

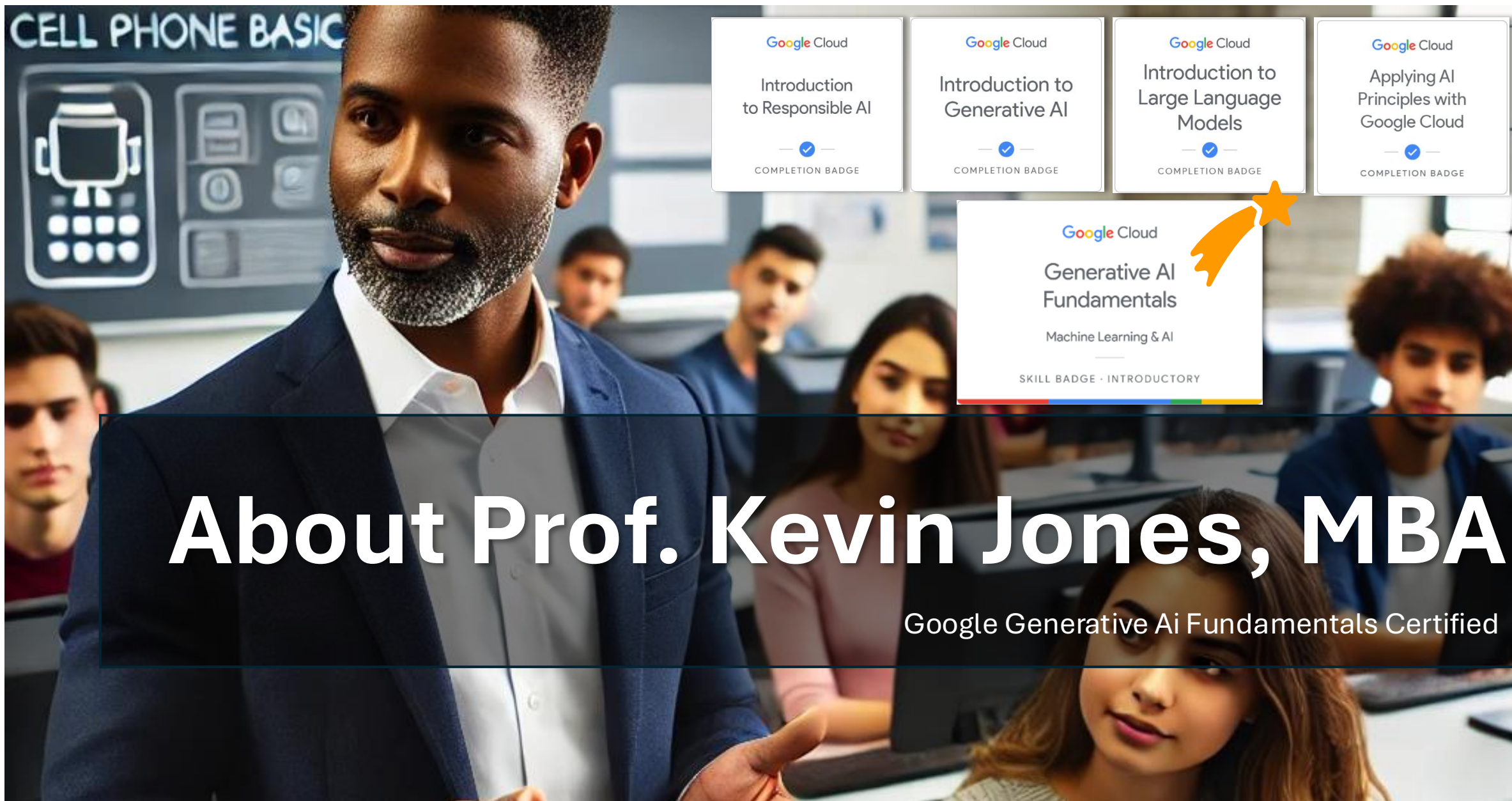
- A basic understanding of AI and how it works.
- Understanding basic AI security concerns.
- Review of online & device specific AI Tools.



Outline

3 hours

- About Prof. Jones
- AI Defined
- Understanding What AI is and is not
- Using AI to simplify your life
- AI Prompts Defined
- Examining Security Issues
- Q&A and Wrap-Up



About Prof. Kevin Jones, MBA

Google Generative Ai Fundamentals Certified

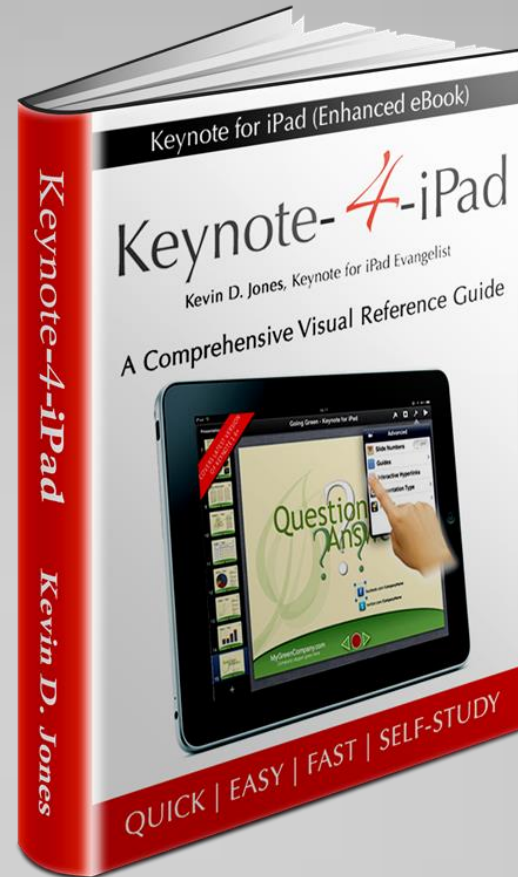
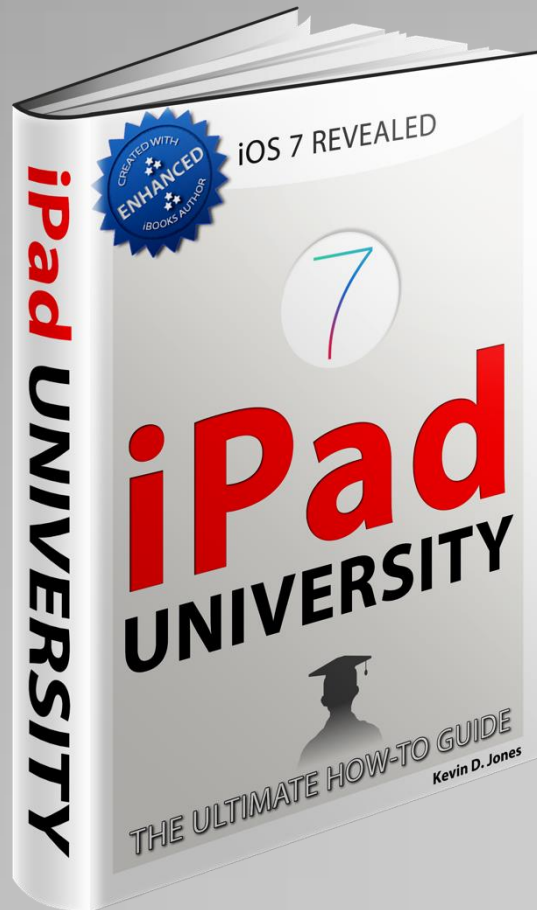
Prof. Kevin D. Jones



- **BS Computer Engineering (PVAMU)**
- **MBA (ISM - Paris, France)**
- **DBA (University of Houston)***
- **Assistant Professor**
Computer Information Technology (CIT)
- **Adjunct Professor**
Business and Information Systems

*Degree completion expected 2026

Award Winning Author



If you aim at nothing, you will hit it every single time.

A man with a grey beard and mustache, wearing a grey sweatshirt with "LONE STAR COLLEGE" and a star logo, stands in a classroom. He is holding a white pen. Behind him is a chalkboard filled with various data visualizations and icons. The chalkboard includes a line graph with an upward arrow, a bar chart, a pie chart, a clock, a target, a star, and the word "CLASSEGE".

Artificial Intelligence DEFINED

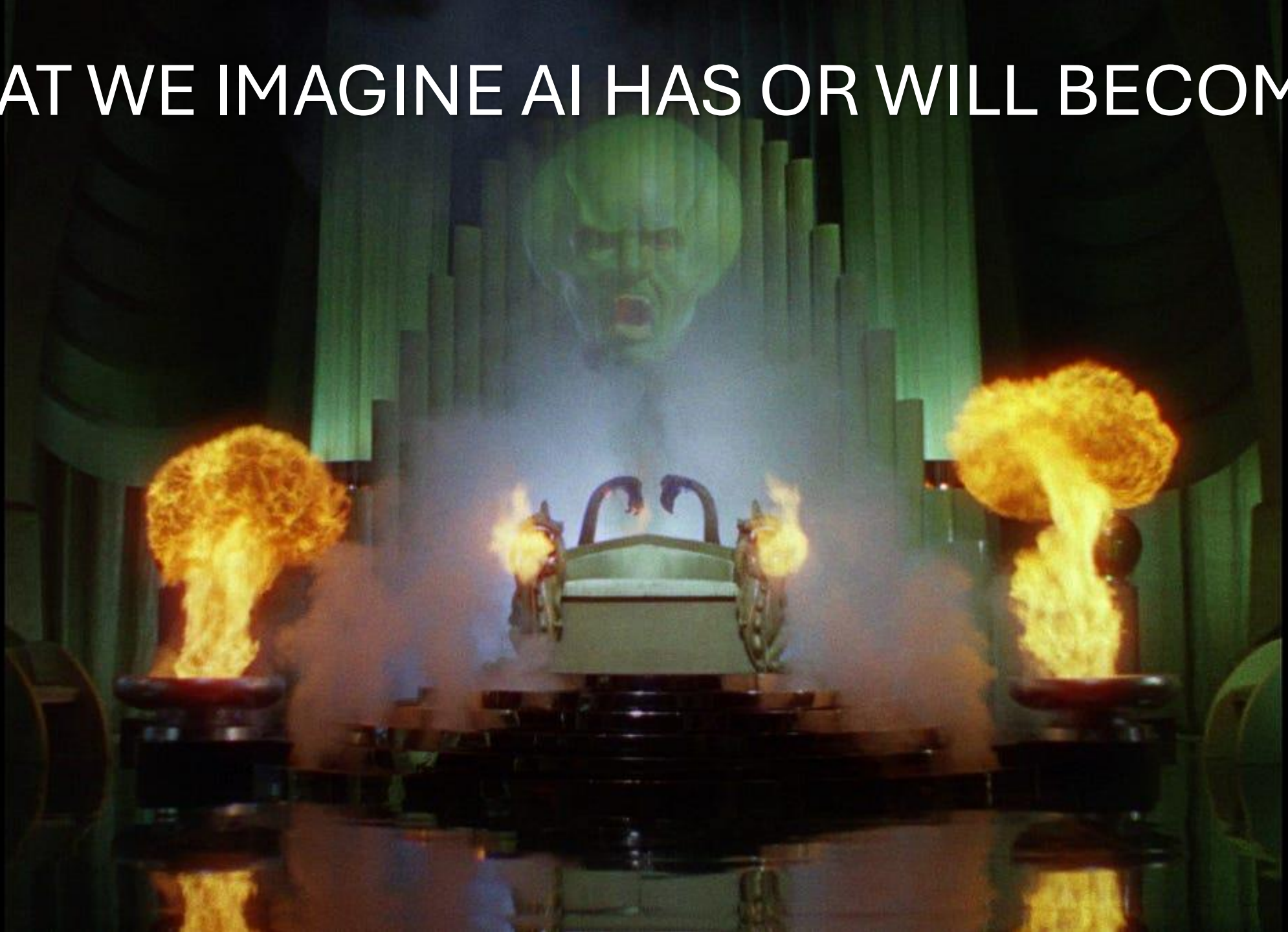
A person with dark hair, wearing a green shirt, is focused on working on a complex piece of machinery. The machine has various components, including red glowing elements and metallic parts. The background is slightly blurred, emphasizing the person and the machine.

Objective: Provide a foundational understanding of what AI is and how it works in simple terms.

Definition of AI:

- **AI** is the ability of a machine to mimic human intelligence, such as learning from data, recognizing patterns, and making decisions.
- **AI systems** are not human but are designed to perform tasks such as problem-solving, language understanding, and visual recognition.

WHAT WE IMAGINE AI HAS OR WILL BECOME...



AS OF OCTOBER 1st 2024



A vertical split-face image. The left side shows a close-up of a female AI character with a pale, translucent blue skin, glowing yellow eyes, and a glowing blue circuit board on her forehead. The right side shows a close-up of a human woman with fair skin, blue eyes, and dark hair. The image is set against a dark background.

AI = NOT HUMAN

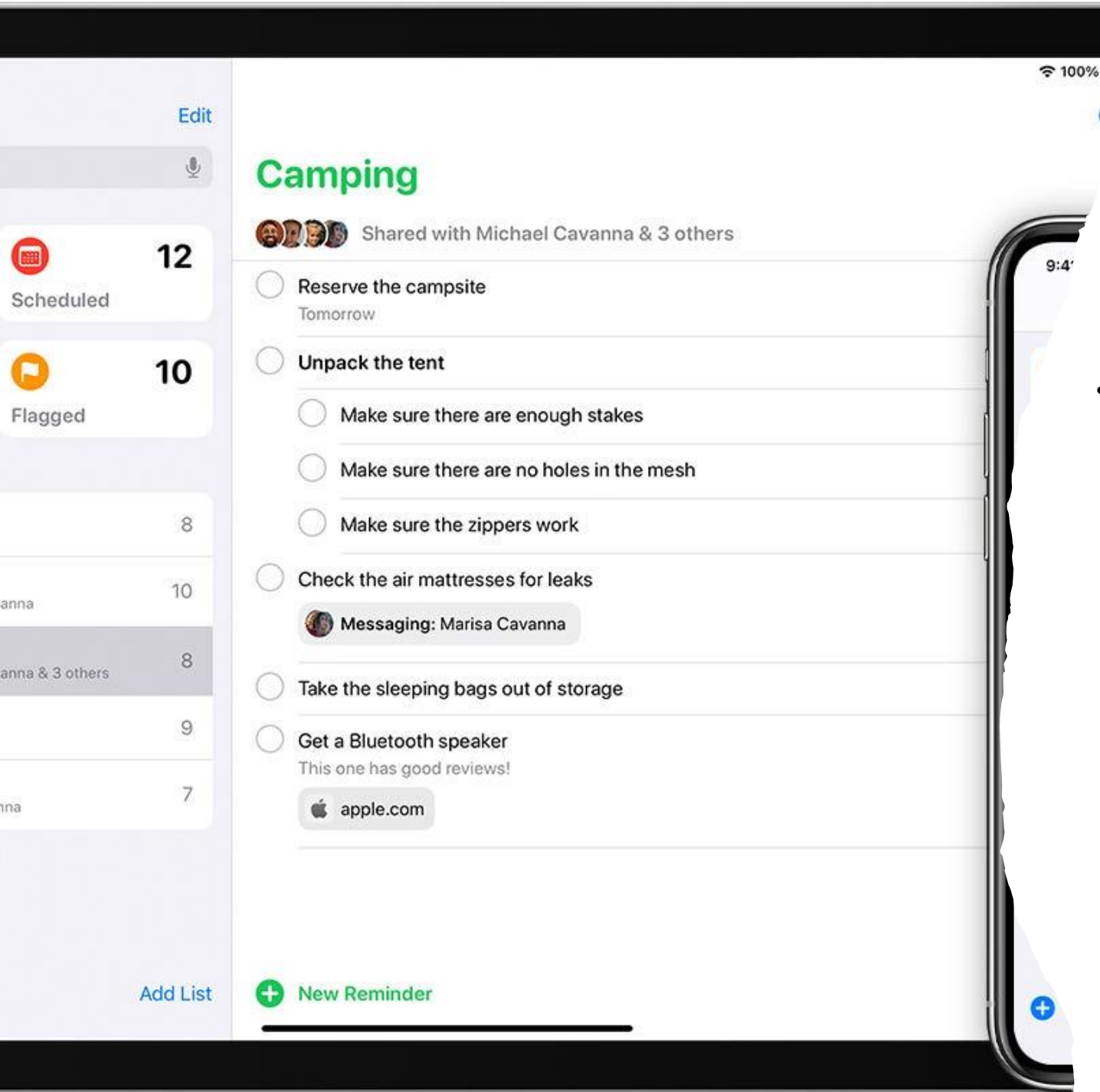
SENTIEN = HUMAN



USING AI to SIMPLIFY YOUR LIFE

Voice Assistants:

- **Siri, Alexa, and Google Assistant** are common examples of AI that respond to voice commands, set reminders, provide answers to questions, or control smart devices.
 - Virtual assistants understand and interpret human speech using NLP, allowing them to process voice commands and respond appropriately. NLP enables them to comprehend context, speech nuances, and intent behind user queries.
-
- Set an alarm, set a reminder, start a countdown time, place a call



USING AI to SIMPLIFY YOUR LIFE

- **Smart Scheduling & Reminders:**
 - Use apps like **Google Calendar** or **Apple Reminders** to automate scheduling and remind you about important events or tasks.



Sending A Message

“Hey Siri, send “persons name” a voice message.”

Note: Default, will disappear after 2 minutes

“Hey Siri, send “persons name” a message.”



Emails

“Hey Siri, send an email to “persons name”

Note: You will be prompted for for subject and message.

“Hey Siri, show me all emails from “persons name”

“Hey Siri, show me all unread emails



Passwords

**“Hey Siri, show me my password for
“application name”**

***Note: You will have to tap on the area
to see the password***



The Weather

“Hey Siri, show me the weather for today”

Note: The more specific you are, the more detailed data you will recv.

“Hey Siri, show me the hourly weather/temperature/rain for “Carthage, Tx” today”



Translation

“Hey Siri, how do you say “where is the bathroom in French”

Note: The more specific you are, the more detailed data you will recv.



Making Phone Calls

“Hey Siri, call “person name” on speaker

Note: You can also end the call if you activate Siri



Finding People & Things

“Hey Siri, where is my “Mac Book Pro”

***Note:** The more specific you are, the more detailed data you will recv. It will also locate airtags.*

“Hey Siri, where is my “person name”

“Hey Siri, where is my “car”

***Note:** You must turn on this feature in maps (Show parked location) is toggled on*



Share Your Location

**“Hey Siri, share my location with
“Regina Jones”**

***Note:** You can add a message to the message as well.*

“Hey Siri, where am I?”



Take A Screenshot

“Hey Siri, how much is 20% of \$279.53

Note: You can add a message



Basic Math

“Hey Siri, take a screen shot and send it to “persons name”

***Note:** You can add a message also*



Time

“Hey Siri, how long until “time”

Note: You can add a message also

“Hey Siri, how many days until “date”

“Hey Siri, set a timer for “30 mins”

“Hey Siri, set a timer an alarm for “3:30 today”



Planning

“Hey Siri, am I free on Friday

***Note:** You can add a message also*

“Hey Siri, am I free on Tuesday ay 10:30a



Setting Meetings and Reminders

“Hey Siri, create a meeting on this Friday and 10:30a

***Note:** You can add a message also*

“Hey Siri, am I free on Tuesday ay 10:30a



USING AI to SIMPLIFY YOUR LIFE

- **AI in Healthcare:**
 - **Wearable devices** like the Fitbit or Apple Watch use AI to monitor your heart rate, track physical activity, and even provide health insights based on patterns.



USING AI to SIMPLIFY YOUR LIFE

- **AI in Home Automation:**
 - Smart home systems like **Alexa**, **Nest** or **Philips Hue** let you control your thermostat or lights using AI, simplifying energy use and comfort.

Physics

Thermodynamics

Artificial Intelligence

MACHINE LEARNING

DEEP LEARNING

DISCRIMINATIVE

LLM's
Large Language Models

Generative AI
Generative Artificial
Intelligence

Artificial Intelligence (AI)

AI: refers to the simulation of human intelligence in machines that are programmed to think, learn, and perform tasks autonomously or semi-autonomously. These tasks include problem-solving, decision-making, language understanding, and pattern recognition. AI systems can either be rule-based or involve learning from data to improve their performance over time.

Machine Learning (ML): A subset of AI that allows systems to learn and improve from experience without being explicitly programmed.

Deep learning is a subset of machine learning that uses neural networks with multiple layers (hence "deep"). It mimics the way the human brain processes information and is especially effective in recognizing patterns in complex, unstructured data like images, sound, and text. Deep learning powers applications like facial recognition, natural language processing, and autonomous driving.

Large Language Models are a type of AI trained on vast amounts of text data to understand and generate human-like language. These models, like GPT-4, are designed to perform various language tasks, such as answering questions, summarizing text, or even generating coherent written content. They use deep learning techniques and can process context and nuance in language more effectively than traditional models.

MACHINE LEARNING

DEEP LEARNING

DISCRIMINATIVE

LLM's
Large Language Models

Generative AI
Generative Artificial
Intelligence

Artificial Intelligence

MACHINE LEARNING

DEEP LEARNING

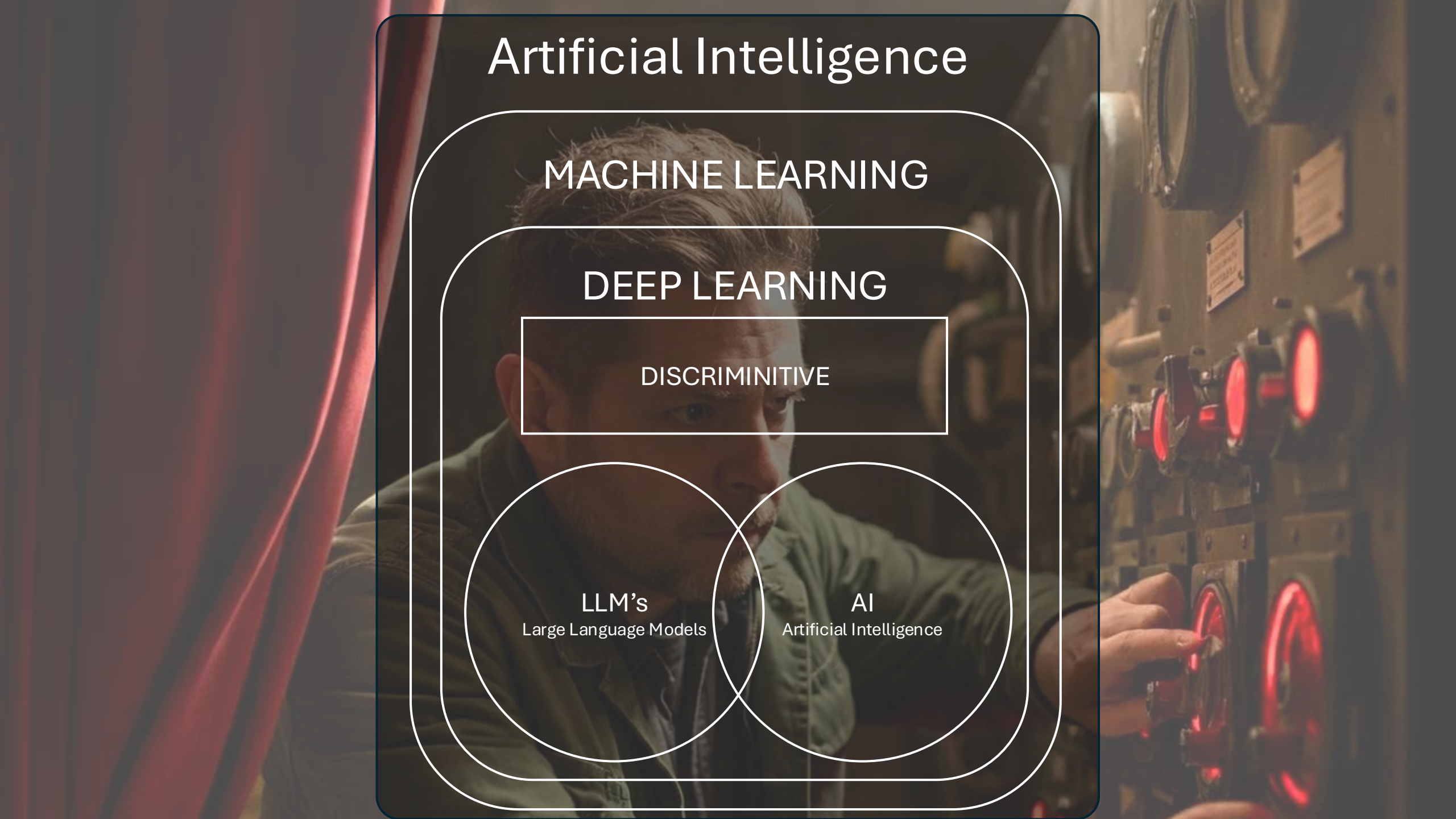
DISCRIMINATIVE

LLM's

Large Language Models

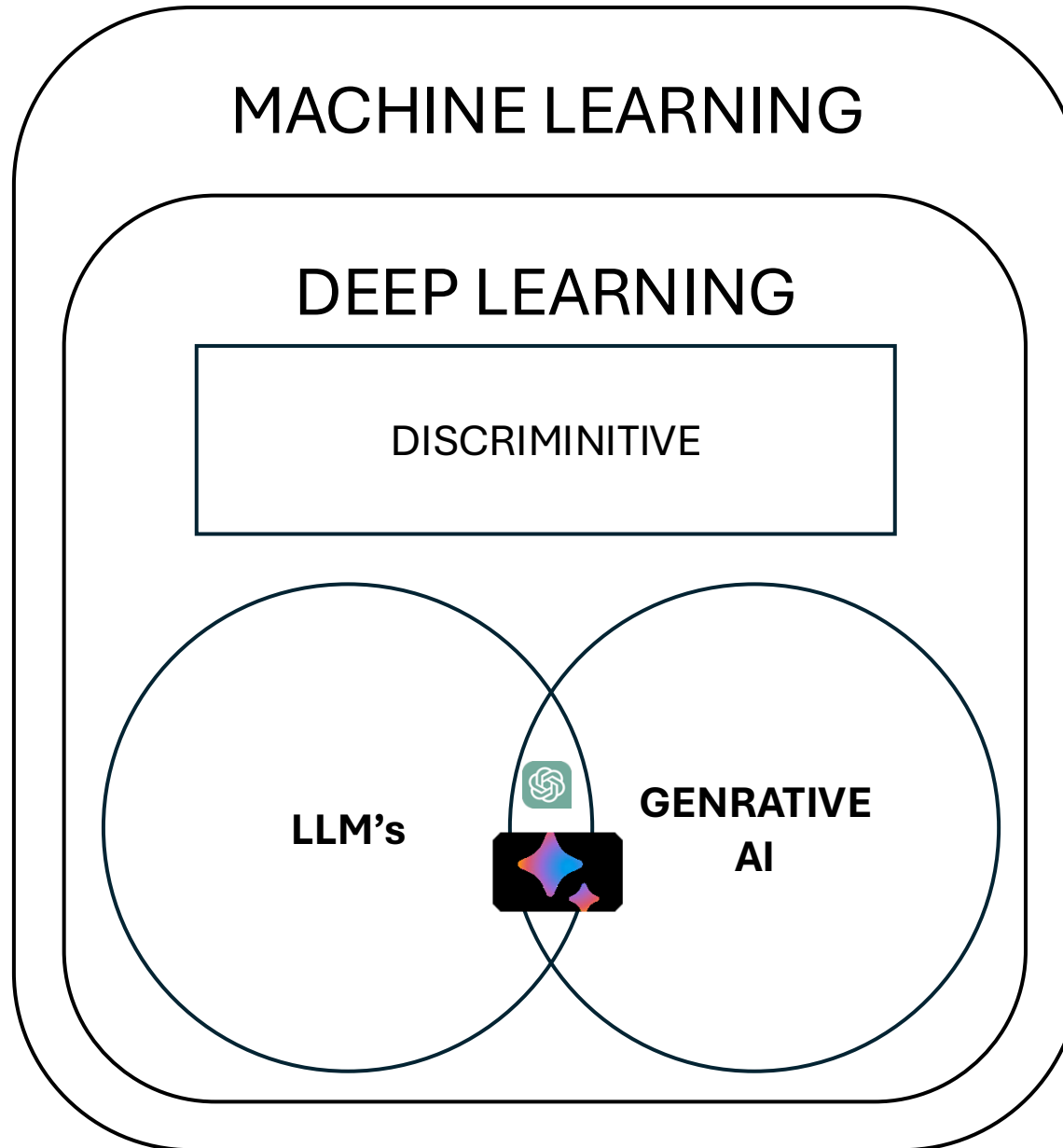
AI

Artificial Intelligence



Artificial Intelligence

- **Algorithms:** A set of rules or instructions that AI follows to perform tasks or make predictions.
- **Data:** The fuel for AI, used to train and improve machine learning models.



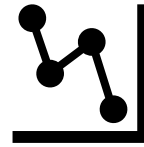
Artificial Intelligence

MACHINE LEARNING

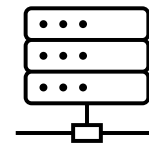
SUPERVISED

UNSUPERVISED

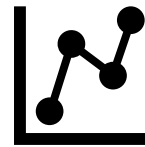
Training Data



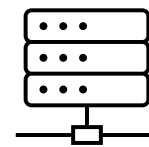
Model



New Data



Trained Model



Predictions



Artificial Intelligence

MACHINE LEARNING

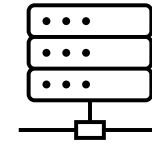
SUPERVISED

UNSUPERVISED

Nike Sales Data



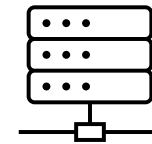
Model



Adidas sales data



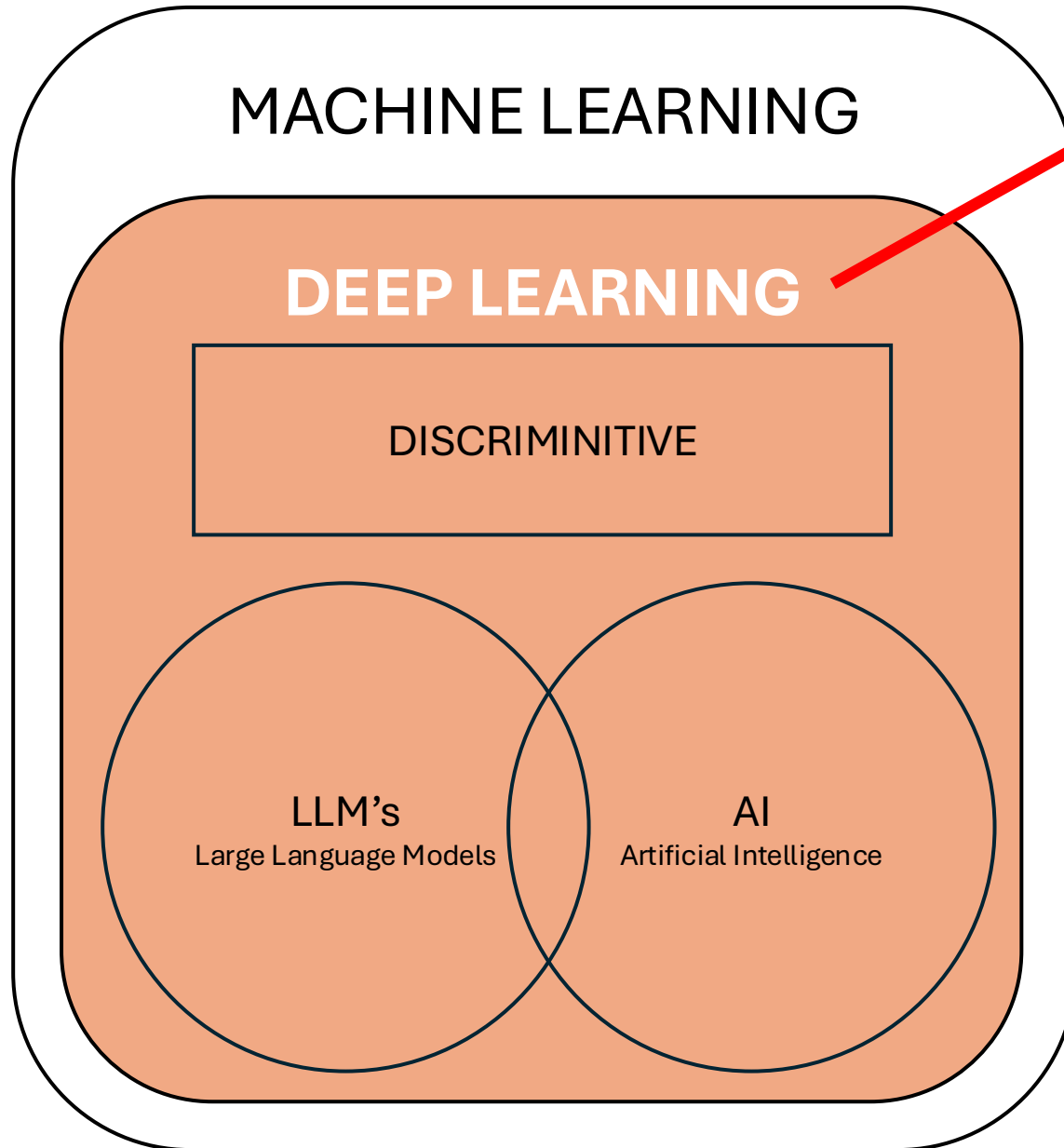
Trained Model



Predictions



Artificial Intelligence



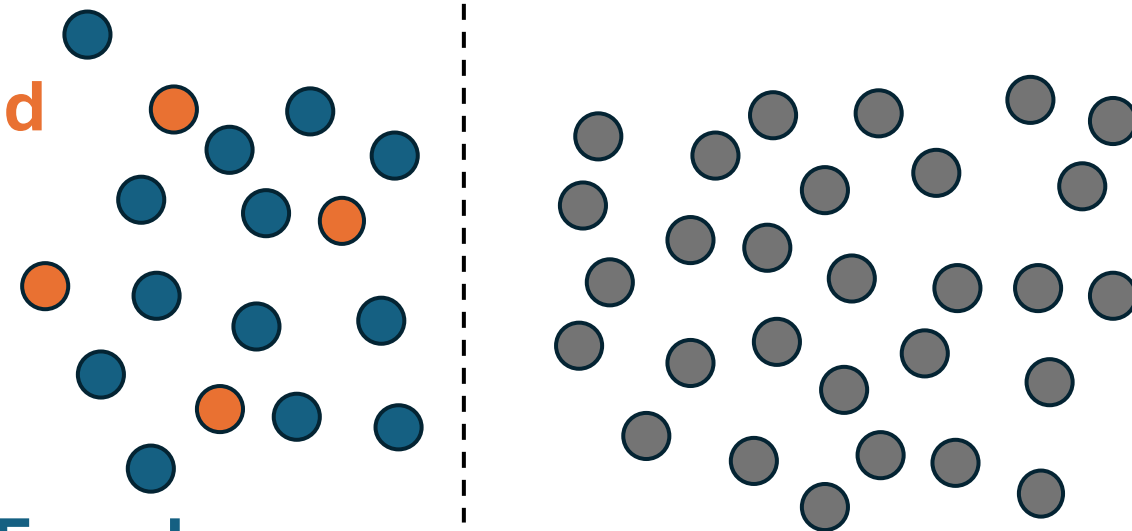
+ Deep Learning Model = Fraud

Fraud

Not Fraud

(labeled Data)

(unlabeled Data)





+ Deep Learning Model = Fraud

MODEL MAKES PREDICTIONS

Fraud

Not Fraud

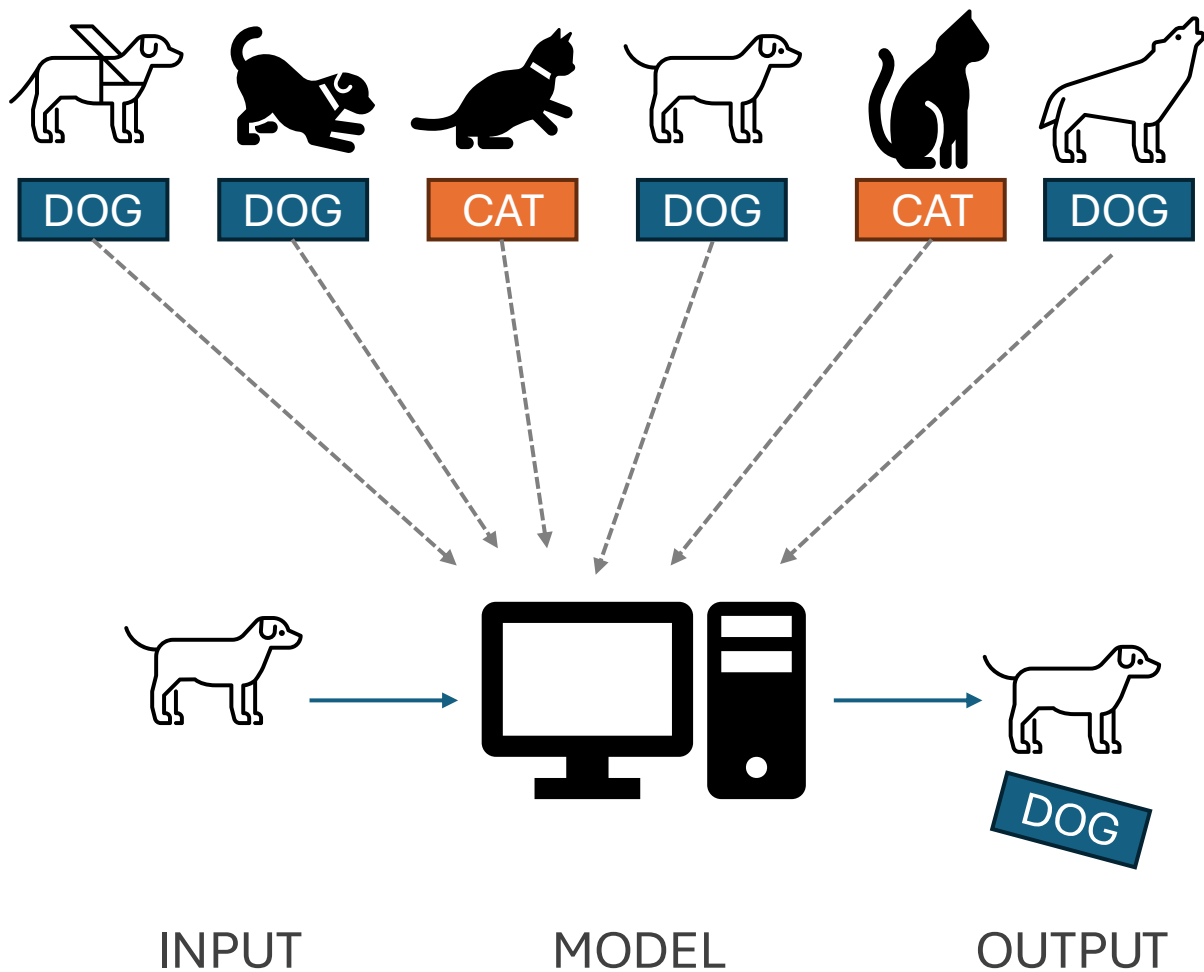
(labeled Data)

Pseudo-Bad

Pseudo-Good

(unlabeled Data)

DISCRIMINATIVE MODEL EXAMPLE



Artificial Intelligence

MACHINE LEARNING

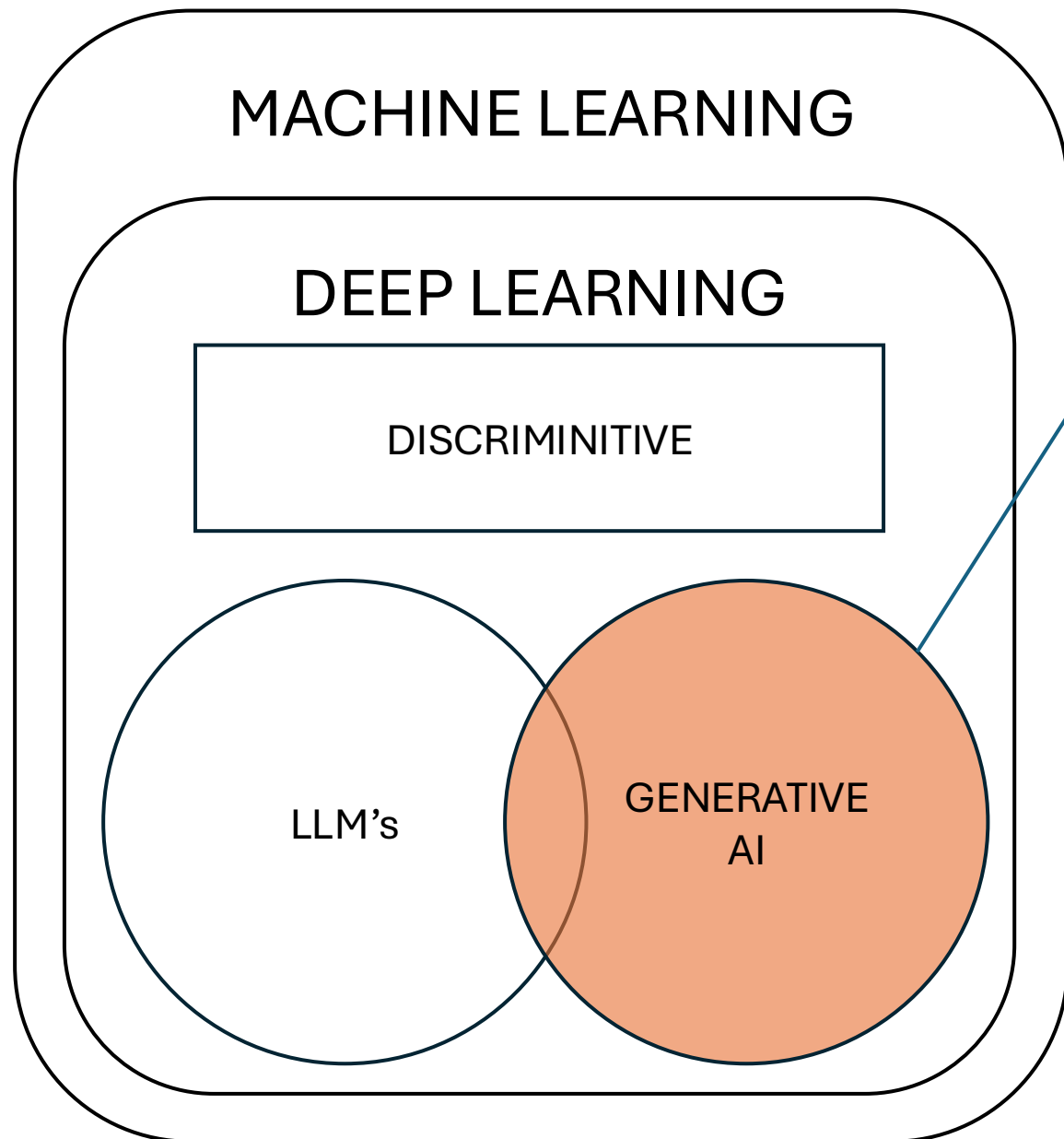
DEEP LEARNING

DISCRIMINATIVE

LLM's
Large Language Models

GENRATIVE AI
Artificial Intelligence

Artificial Intelligence



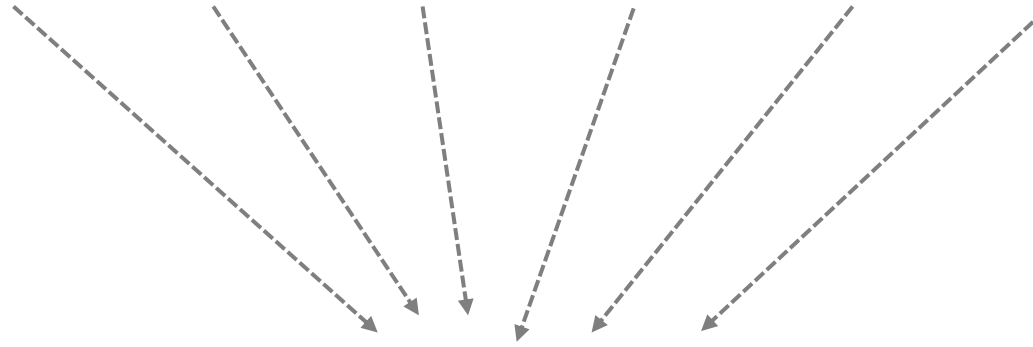
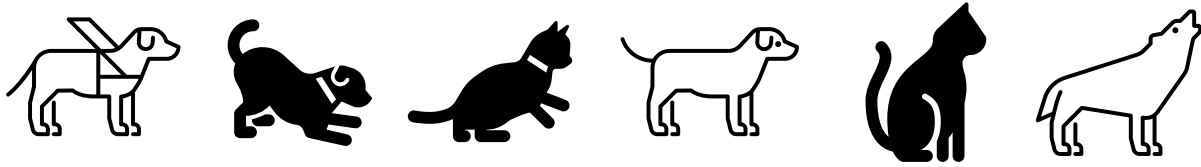
GENERATIVE LEARNING MODELS

↓
TEXT INPUT (e.g. prompt)

↓
GENERATIVE MODELS
Learn about the patterns in
the training data

↓
Generates something
completely new based on
the patterns

GENERATIVE MODEL EXAMPLE



Give me an
image of a dog



PROMPT

MODEL

OUTPUT

Artificial Intelligence

MACHINE LEARNING

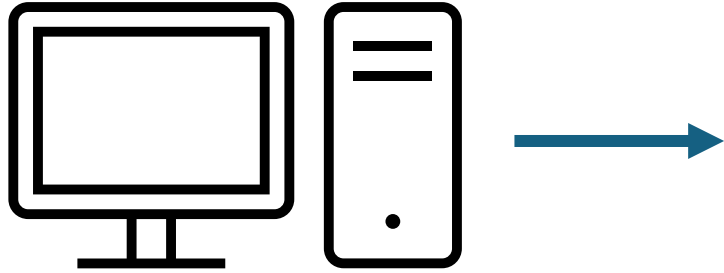
DEEP LEARNING

DISCRIMINATIVE

LLM's
Large Language Models

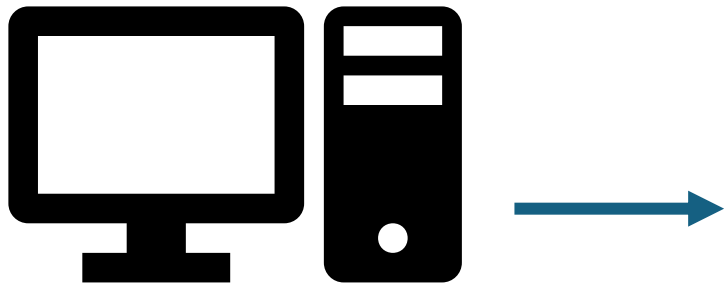
GENERATIVE AI
Artificial Intelligence

GENERATIVE AI (YES or YES)



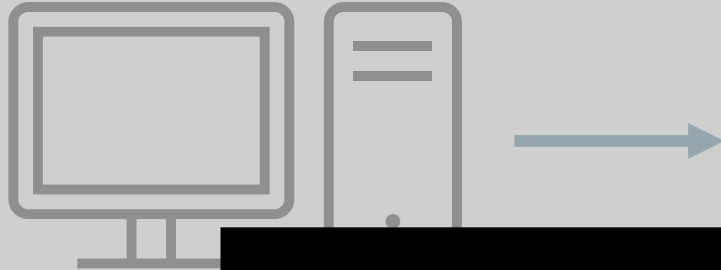
It's Not GenAI:

1. Number
2. Classification (e.g. spam or not spam)
3. Probability



It Is GenAI:

1. Natural Language (text to speech)
2. Images
3. Audio
4. Video



It's Not GenAI:

1. Number
2. Classification (e.g. spam or not spam)

GENERATIVE AI GENERATES NEW SAMPLES THAT ARE SIMILAR TO THE DATA IT WAS TRAINED ON



It IS GenAI:

1. Natural Language (text to speech)
2. Images
3. Audio
4. Video

GENERATIVE AI MODEL TYPES

Text-to-text

Take natural language input and produce text output



ChatGPT



Google Bard

Text-to-image

Trained on large set of images, and generate new images



Text-to-video

Can generate and edit videos



Text-to-3D

Can be used to produce gaming assets



Text-to-Task

Trained to perform a specific task or action based on text input



Google Bard

LARGE LANGUAGE MODELS (LLM's)

Pre-trained with a very large set of data, then **fine-tuned** for specific purposes.

Artificial Intelligence

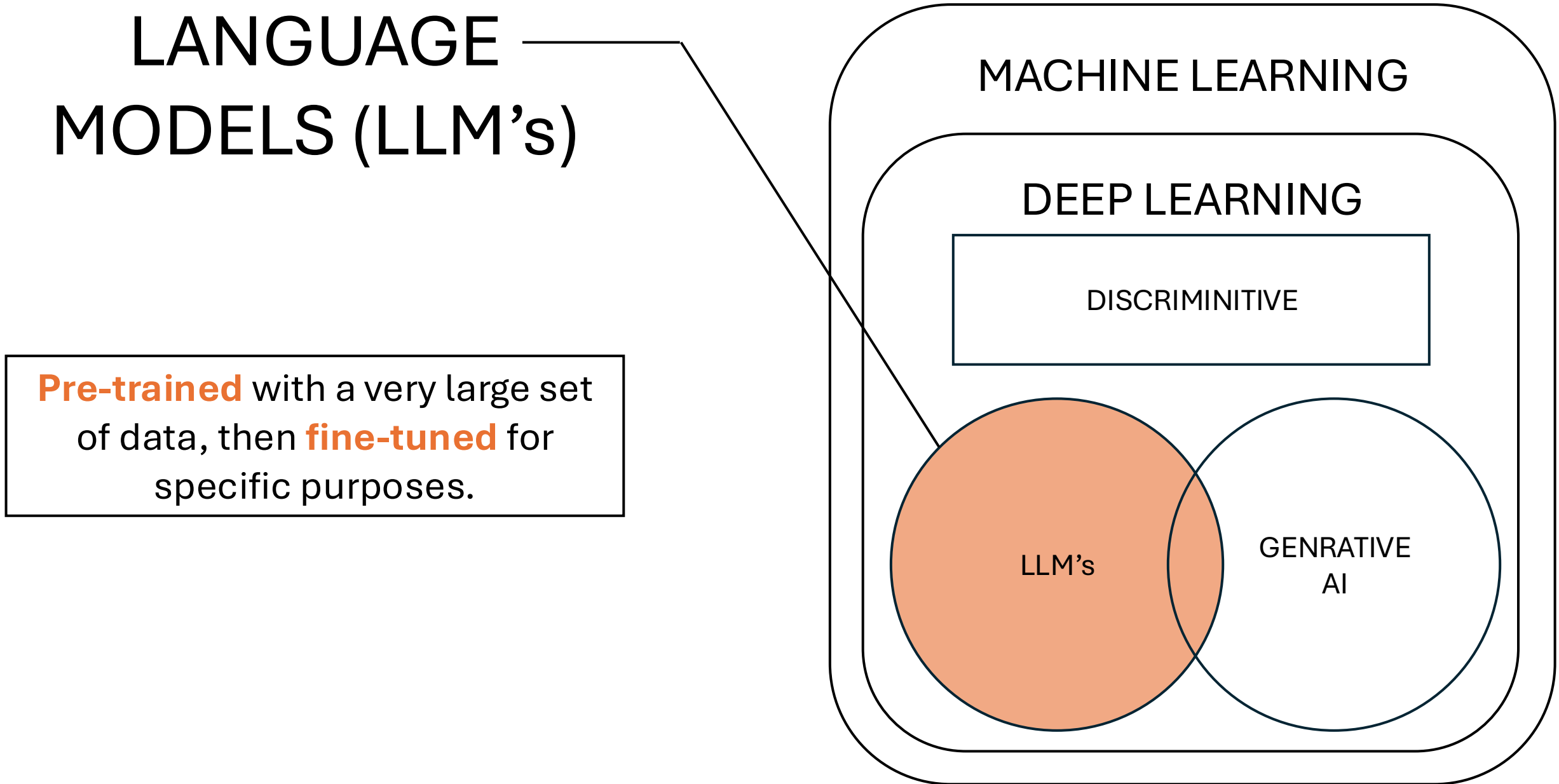
MACHINE LEARNING

DEEP LEARNING

DISCRIMINATIVE

LLM's

GENRATIVE
AI



LARGE LANGUAGE MODELS (LLMs)

Pre-trained

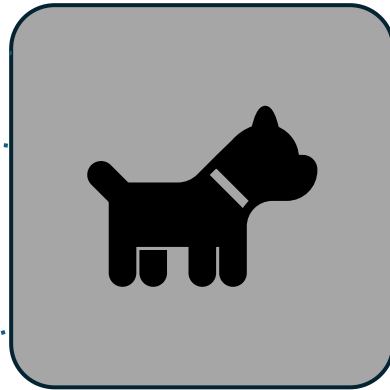
Fine-tune

Sit

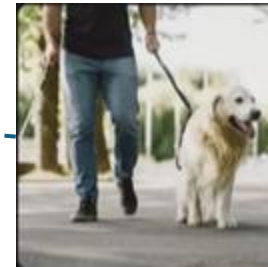
Come

Down

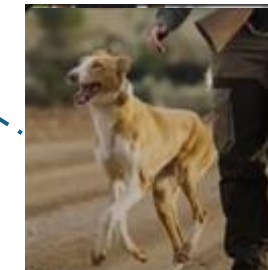
Stay



Police Dog



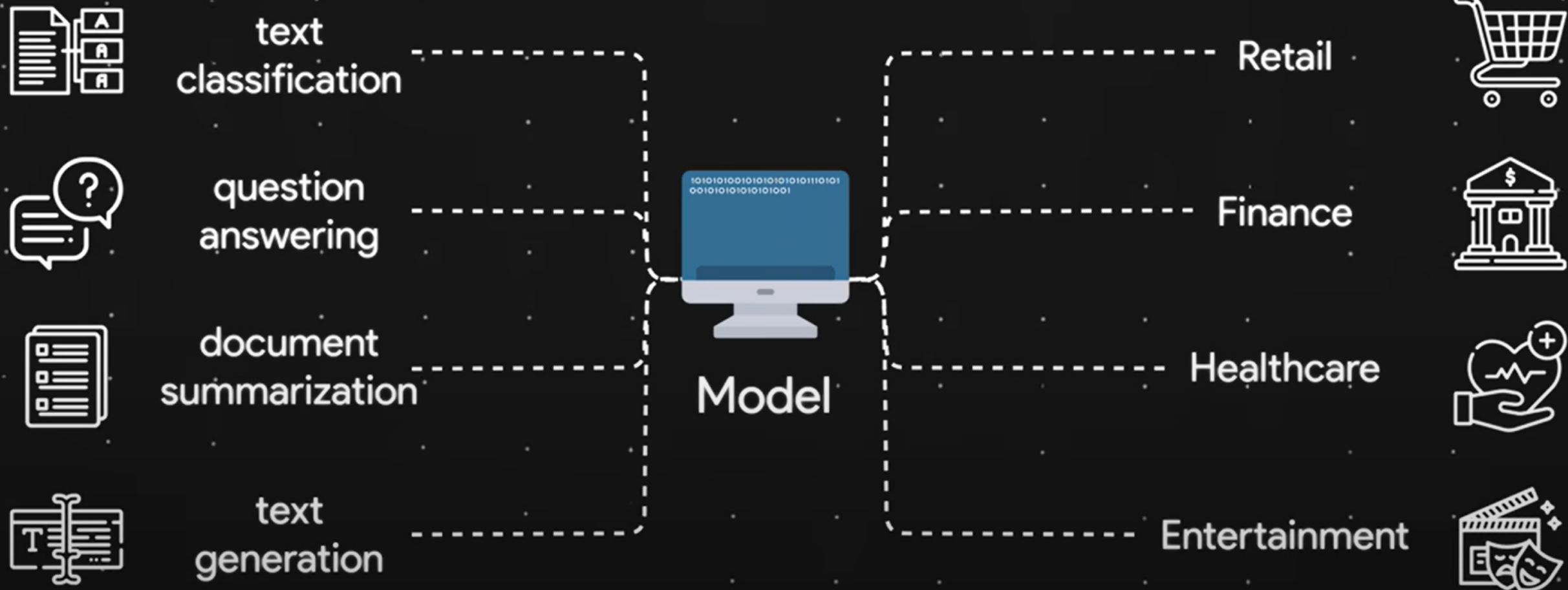
Guide Dog






Hunting Dog

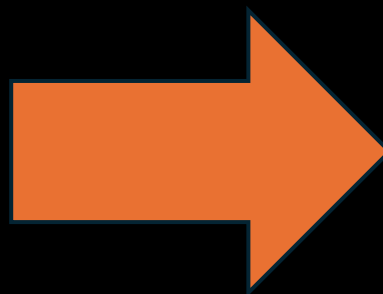
Pre-Trained

Fined-Tuned



LLMS: REAL WORLD EXAMPLE

1. Hospital buys pre-trained LLM from:

2. Hospital fine-tunes LLM with it's own medical -specific data
3. Hospital uses LLM to improve diagnostic accuracy



The 3 Types of AI Tools

Standalone AI Tools

AI powered software designed to work **independently with minimal setup**.



Tools With Integrated AI Features

Built-in AI enhancements within a particular piece of software



Custom AI Solution

An application that's **tailor-made to solve a specific problem**.



Developed a custom solution to detect [sepsis](#). Improved detection from 2% – 5% to up to 40%.

Artificial Intelligence



ChatGPT



Google Bard

Technology that powers LLM
Chatbots like ChatGPT and
Google Bard

MACHINE LEARNING

DEEP LEARNING

DISCRIMINATIVE

LLM's

GENRATIVE
AI



A close-up, slightly blurred photograph of a man with dark hair and glasses, looking down. The background is out of focus, showing what appears to be an indoor setting with lights and other people. A large white number '2' is overlaid on the left side of the image.

2

UNDERSTANDING **WHAT IS AI** & **WHAT AI IS NOT?**



Understanding What is AI & What AI is Not?

- **Objective:** Address common misconceptions about AI and explain what AI can and cannot do.

Understanding What is AI & What AI is Not?

- **What AI *Is Not***

- AI is *not* sentient. It doesn't think, feel, or make moral decisions.
- AI is *not* a human replacement for all jobs or tasks; it assists with tasks that require repetitive processing or data analysis.



Understanding What is AI & What AI is Not?

- **What AI Is**

- AI is a tool that performs tasks like recommending products, voice recognition, and filtering spam emails.
- It excels in pattern recognition and large-scale data processing, such as identifying faces in photos or predicting trends in weather or markets.





3

USING AI to **SIMPLIFY**
YOUR LIFE

A man with short brown hair and a beard, wearing a white and tan striped polo shirt, is leaning over a white desk in a computer store. He is looking intently at a computer monitor. The background is filled with rows of computer monitors on shelves, many of which display a blue screen with a green tree logo. To the right, there are shelves with various computer peripherals like headphones and mice. A large white number '4' is overlaid on the left side of the image.

4

AI PROMPTS DEFINED



AI PROMPTS DEFINED

- **What are AI Prompts?**
 - AI prompts are instructions or inputs you give to an AI system (like a chatbot or image generator) to achieve a desired response or result.
- **Why Prompts Matter:**
 - Well-defined prompts help AI give more accurate and useful outputs. For example, asking an AI assistant “Remind me to take my medicine every morning at 9 AM” is more effective than saying “Remind me later.”



AI PROMPTS DEFINED

- **Examples of Good vs. Bad Prompts:**
 - **Good Prompt:** “Find Italian restaurants within 5 miles that are open now.”
 - **Bad Prompt:** “What’s for dinner?”
- **Practical Tips for Writing Effective Prompts:**
 - Be specific and clear in your instructions.
 - Include relevant details like time, place, or context.



AI PROMPTS DEFINED

GIGO - Garbage In Garbage Out

Write prompts that are clear and provide context. Start with an action word and state the desired outcome.

- **Ok Prompt:** Write a haiku.
- **Better Prompt:** Write a humorous haiku for my friend who likes dragons.

The same prompt won't always produce the same result. Try refining the prompt one word at a time or gradually adding complexity to get the results you want. Since many chat ai programs remember your previous chats you can build on those. Always check the output to verify that it is accurate.



AI PROMPTS DEFINED (RTF)

1. Simplifying Complexity: The RTF Framework

Being the most widely-used framework due to its intuitive nature, RTF harnesses three pivotal points:

- Role
- Task
- Format

It functions as a universal tool for crafting prompts, simplifying them into a question, such as: “Act like a [role]. Can you [insert task] in [format] format?” Such a structure is not only easy to remember but also effortlessly applicable across varied scenarios, ensuring improved, tailored outputs.

Example:

“Act like a skilled carpenter. Can you guide me through building a laptop stand using wood in a step-by-step instruction format?”

Outcome:



AI PROMPTS DEFINED (RODES)

Meticulous Outputs with RODES

The **RODES** framework shines, especially when examples similar to the anticipated output are at hand:

- **Role**
- **Objective**
- **Details**
- **Examples**
- **Sense Check**

Leveraging the **RODES** framework, the model is well-guided through the task with clear objectives, detailed information, real-life examples, and a final checkpoint to ensure the output aligns seamlessly with the expectations.

Example:

Taking on the Role of a master woodworker, help me to define a clear Objective in creating a functional laptop stand, offering all relevant Details and Specifics, perhaps providing Examples of similar designs, and conducting a Sense Check to ensure practicality and feasibility in a home woodworking setting.



How would you speak to a 5 year old learning to ride a bike?



5

Examining Security Issues & Errors

AI

Hallucinations
&
Risks



1. Data Privacy and Security Risks

Issue: AI tools like ChatGPT process vast amounts of user data, including personal and sensitive information. If this data is not properly secured, it could be exposed to cyberattacks or unauthorized access.

Risk: Users may unintentionally share personal or confidential information, such as financial details, in their interactions with AI, which could be stored or logged by the service provider. This poses a privacy risk, especially if the data is not adequately protected or anonymized.

Example: If a user asks an AI chatbot for financial advice and provides sensitive information, this data could be compromised if the system experiences a breach.

Source: [*OpenAI Privacy Policy*](#)

2. AI Systems Vulnerability to Hacking

Issue: AI systems can be vulnerable to attacks such as **data poisoning** (feeding malicious data to AI models) or **model inversion** (attempts to reverse-engineer the training data used in AI models). Hackers could exploit these vulnerabilities to gain access to confidential information or manipulate the AI's responses.

Risk: Hackers could exploit weaknesses in the AI model to alter its behavior or access the sensitive data it has processed or stored.

Example: By manipulating the training data, attackers could influence how an AI tool behaves or responds, leading to incorrect or harmful outputs.

Source: *Forbes - AI Security Vulnerabilities*

3. Phishing and Social Engineering

Issue: AI tools like ChatGPT can be used for social engineering or phishing attacks, where malicious actors use the AI to create convincing fake messages, emails, or content that trick users into providing sensitive information.

Risk: Malicious use of AI-generated content can lead to identity theft, financial fraud, or other security breaches.

Example: An AI could be used to craft highly personalized phishing emails that appear legitimate, increasing the likelihood of users falling victim to scams.

Source: Cybersecurity and Infrastructure Security Agency (CISA) - Phishing Threats

4. AI Bias and Misuse

Issue: AI tools are only as good as the data they are trained on. If the training data contains biases or inaccuracies, the AI may reflect or amplify these biases in its responses. Malicious actors could exploit these biases to generate harmful or misleading content.

Risk: In sensitive contexts, biased or incorrect AI outputs could harm users by providing inaccurate or inappropriate information, especially in areas like healthcare, law, or finance.

Example: An AI tool may disproportionately favor or disadvantage certain groups based on biased training data, leading to discrimination in automated decision-making processes.

Source: Brookings Institution - AI Bias and Security



5. Lack of User Control and Transparency

Issue: Users may not fully understand how AI tools like ChatGPT work, what data they collect, and how this data is used. AI models often function as "black boxes," making it difficult to audit or understand the decision-making processes behind them.

Risk: Without transparency, users may unknowingly expose themselves to security risks or be unaware of how their data is being utilized by the AI system.

Example: Users may believe that AI systems are entirely secure, but without understanding the limitations and risks, they may inadvertently share sensitive information or rely on incorrect outputs.

Source: [Harvard Business Review - The Risks of AI](#)

6. Malicious Use of AI for Cyberattacks

Issue: AI tools can be used to automate and scale cyberattacks, such as distributed denial of service (DDoS) attacks, identity theft, or automated hacking attempts. Attackers can use AI to identify vulnerabilities more quickly and launch sophisticated, adaptive attacks.

Risk: AI-driven cyberattacks could be faster and more difficult to detect or prevent, leading to more widespread and effective security breaches.

Example: AI-driven bots could conduct rapid scans of networks and exploit vulnerabilities faster than traditional methods.

Source: ZDNet - How AI is Used in Cyberattacks



7. Mitigation Strategies:

Data Encryption: Ensure that AI tools encrypt data both in transit and at rest to protect it from unauthorized access.

User Awareness: Educate users about what kind of information they should avoid sharing with AI tools, especially in sensitive contexts.

Ethical AI Development: Encourage transparency and accountability in AI development to minimize biases and ensure proper handling of data.

AI Monitoring: Implement robust monitoring to detect any misuse or security vulnerabilities in AI systems. By understanding these risks and adopting proper safeguards, both users and developers can ensure the secure use of AI tools like ChatGPT.

A group of diverse professionals are seated in a meeting room. In the foreground, a man with short dark hair and a beard, wearing a dark suit, is speaking into a silver microphone. He is looking towards the right. Behind him, several other people are visible, including a woman with glasses and curly hair, a man in a grey suit, and a woman with long dark hair. The background is slightly blurred, showing a modern office environment with white walls and some colorful circular decorations.

6

Q & A