# Introduction to Generative Artificial Intelligence


Sarveshwaran R

# Agenda

- Introduction to GenAI
- Need of GenAI
- History of GenAI
- GenAI Tools
- Application of GenAI
- Traditional ML Methods vs GenAI
- How does GenAI work?
- Foundation Models
- Building Blocks of GenAI
- Responsible AI

# Generative AI

**What is Generative AI?**

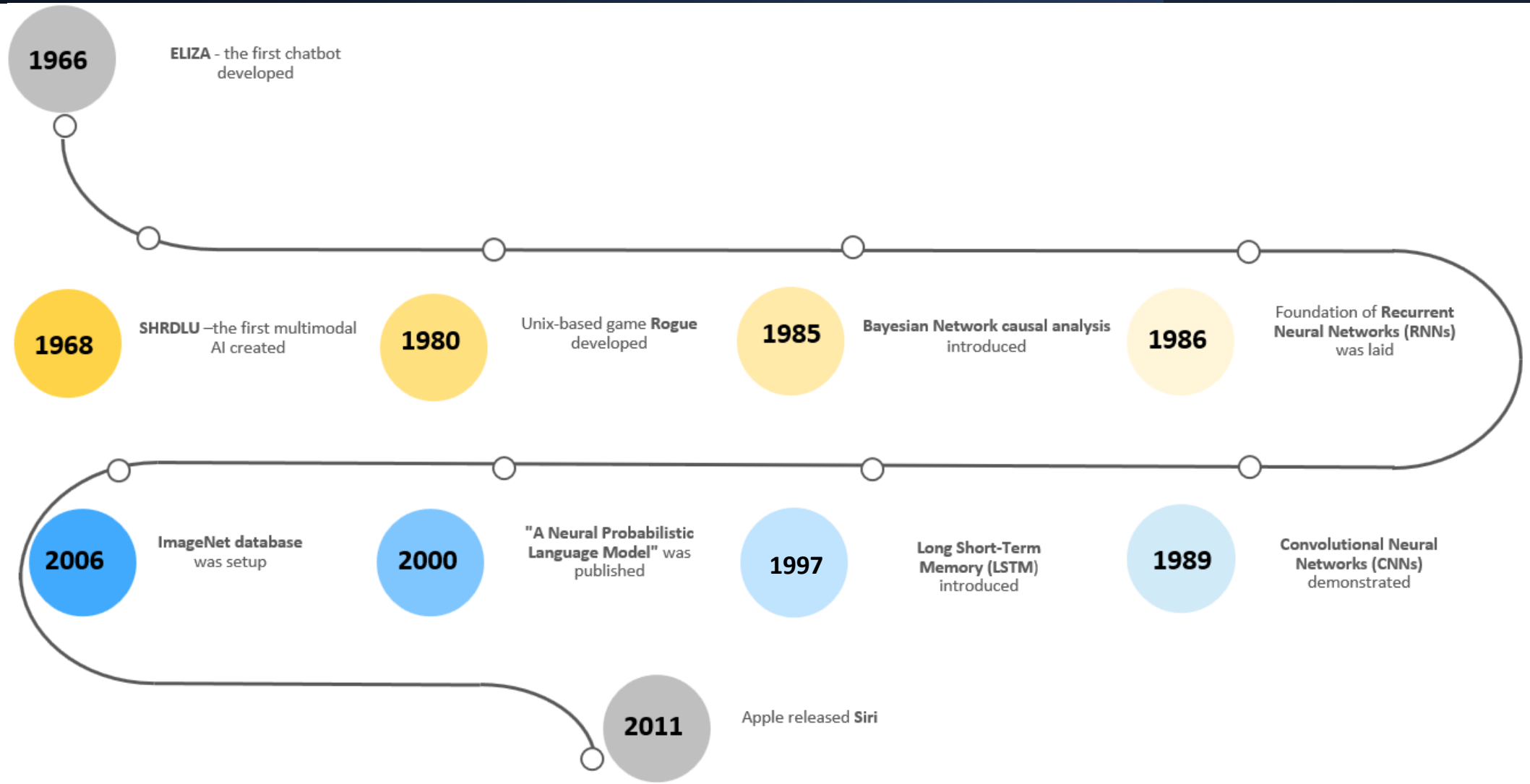
Generative AI is a class of artificial intelligence models that are **capable of autonomously creating content** in the form of **text, images, audio, video** and even **synthetic data.**

**Why Generative AI?**

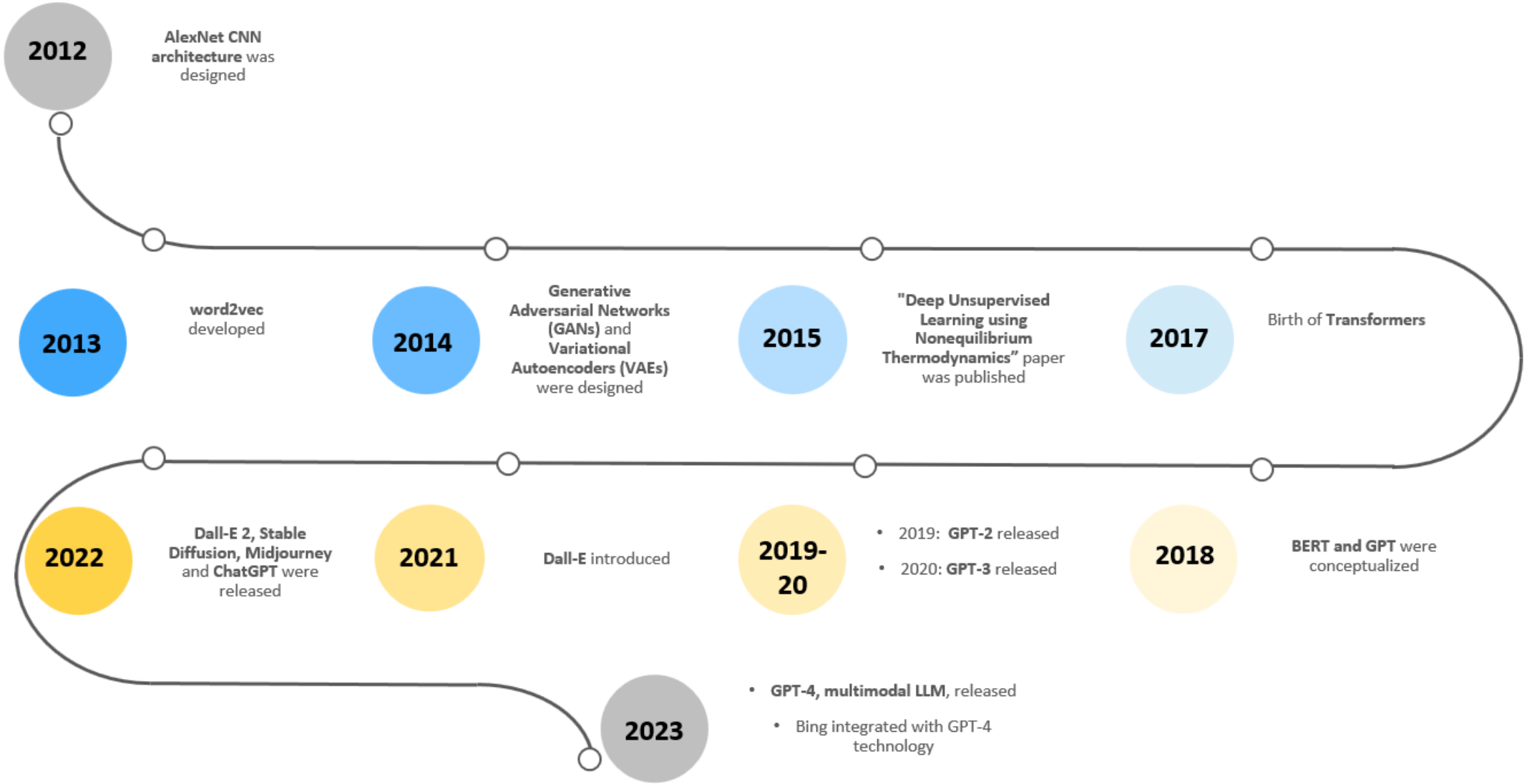
- Faster results
- Improved & original quality content
- Greater Customer Satisfaction
- Increased Efficiency
- Cost reduction
- Improved decision making

NSE talent sprint

# Evolution of GenAI : 1966 - 2011



# Evolution of GenAI : 2012 - 2023



# GenAI Tools

OpenAI's GenAI conversational chatbot. Built on GPT 3.5 generates essays as responses

Google's conversational GenAI chatbot based on LLM, called PaLM

OpenAI's multi-modal text-to-image generator tool creating digital images

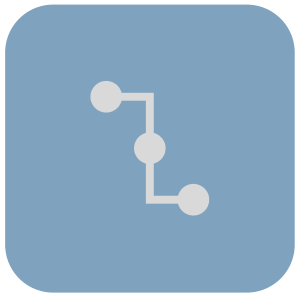
Stable Diffusion, a text-to-image diffusion model and Stable Doodle, a sketch-to-image service to create high-quality images

AI-image generator tool like DALL-E generating images from text inputs. Its output is in an eccentric art-work style

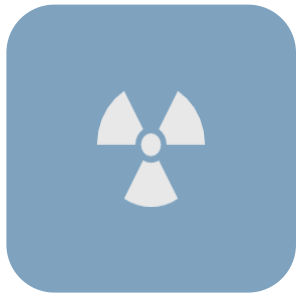
Databricks joined hands with MosaicML to offer generative AI tools

Offers host of foundation models and tools for customization on Amazon's cloud computing platform

# Use Cases of GenAI



Supply Chain



Risk Mitigation & Compliance

Banking & Finance

Surveillance

Retail

Advertising

Manufacturing

Telecom

Gaming

Music

Sports

Healthcare

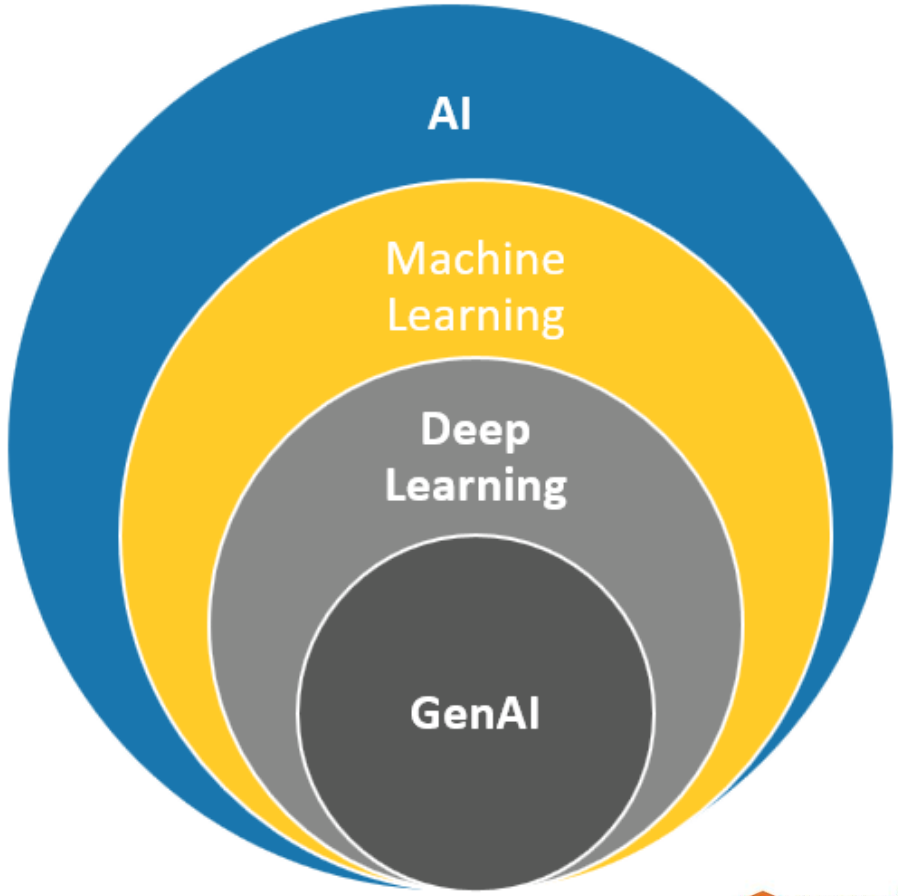
# Traditional ML Methods vs GenAI

**Artificial Intelligence**
Enables machines to mimic human intelligence for performing cognitive tasks

**Machine Learning**
Ability to automatically learn and improve without explicit instructions

**Deep Learning**
Uses multi-layered neural network to self-learn patterns on large data

**GenAI**
Independently generate content in response to prompts.



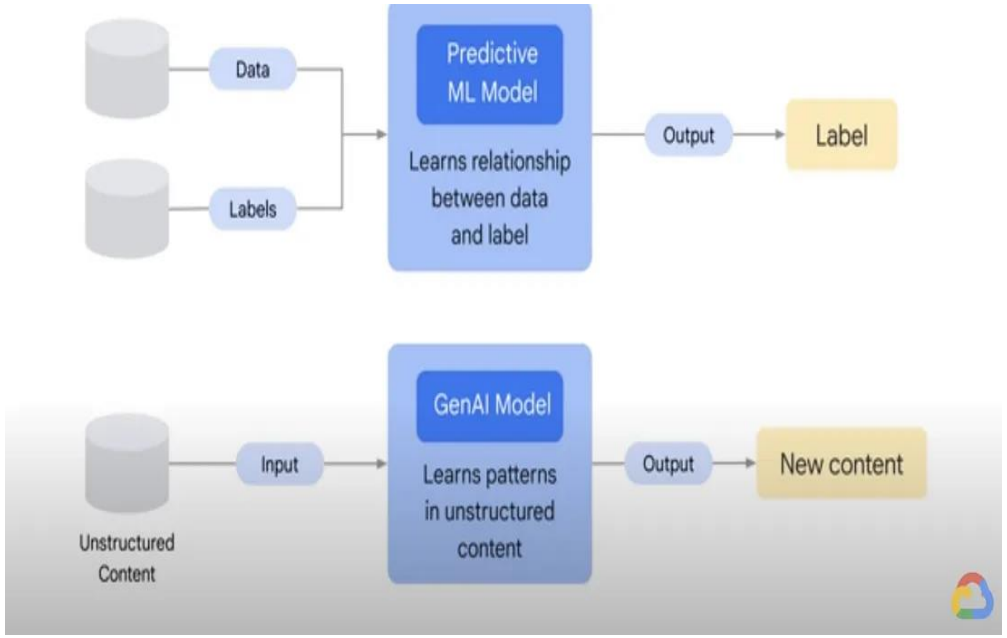

NSE talent sprint

# Traditional ML Methods vs GenAI

- **Traditional ML:** understand data & predict or classify
- **Gen AI:** construct content like train data

- **Traditional ML:** Discriminative | Unidirectional | Label & Unlabeled data
- **Gen AI:** Bidirectional - dual-learning | Unlabeled data | Uni-modal | Bi-modal

- **Traditional ML:** Recommenders, Virtual Assistants, Segmentation, Speech Recognition
- **Gen AI:** creative tasks with customization

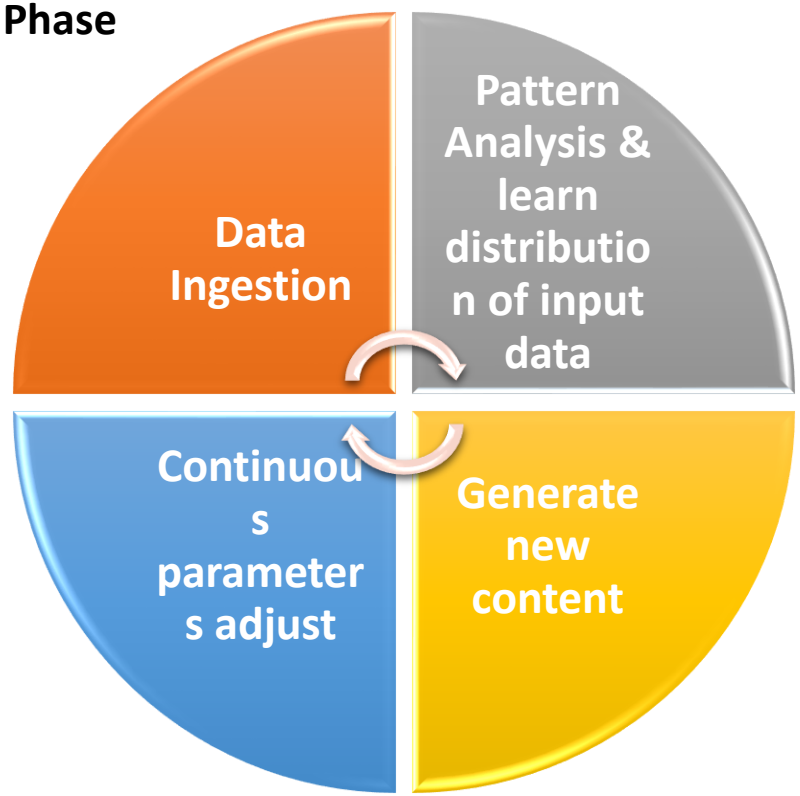



Source: https://medium.com/google-cloud/google-cloud-skills-boost-part-1-introduction-to-generative-ai-4511ec555814

NSE talent sprint

# How does GenAI work?

**Training Phase**



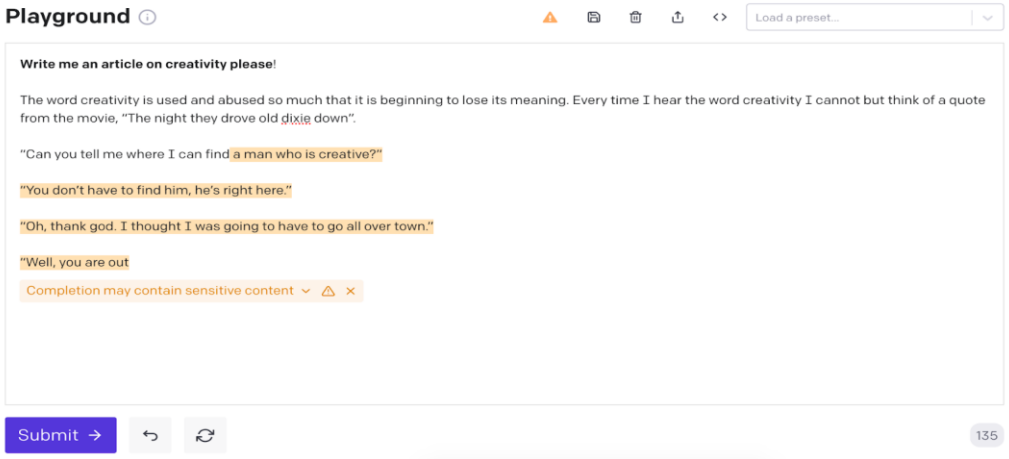

**Inference Phase**


NSE talent sprint

# Foundation Models

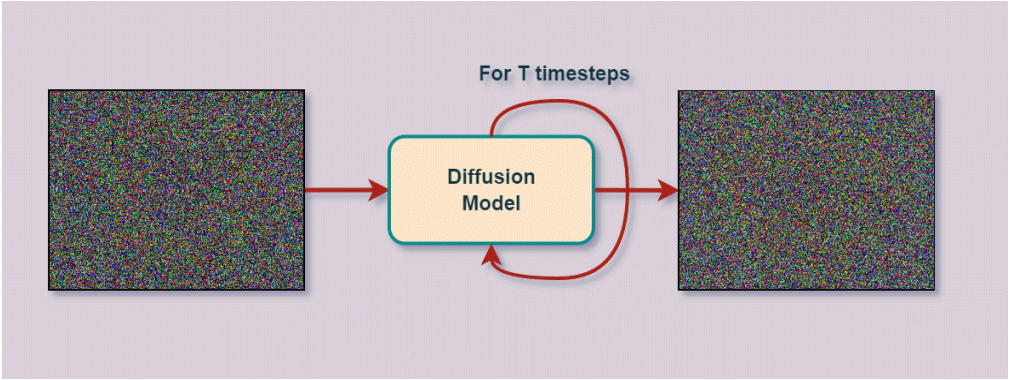
## Generative Pre-Trained

- Large language transformer-based models
- Draws Chat GPT
- Trained on billions of parameters large internet datasets
- Multitude of NLP use cases

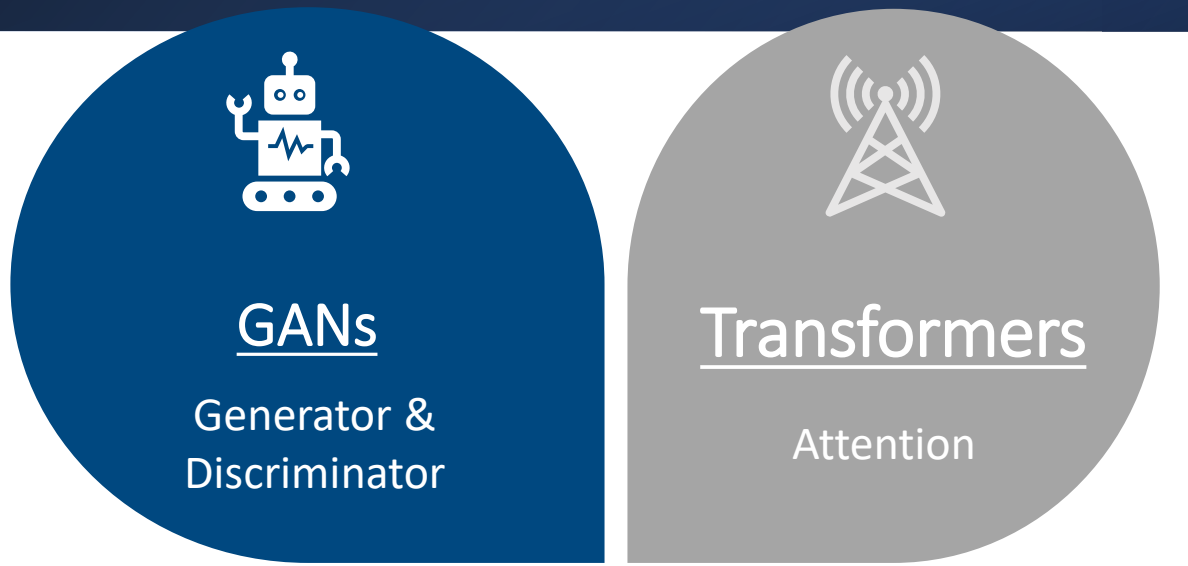



## Diffusion Models

- Deep generative models
- Uses stochastic model: Markov Chain
- Learns structure of a given image by removing the noise or blur

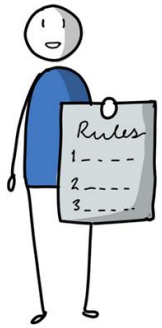


# Building Blocks of GenAI



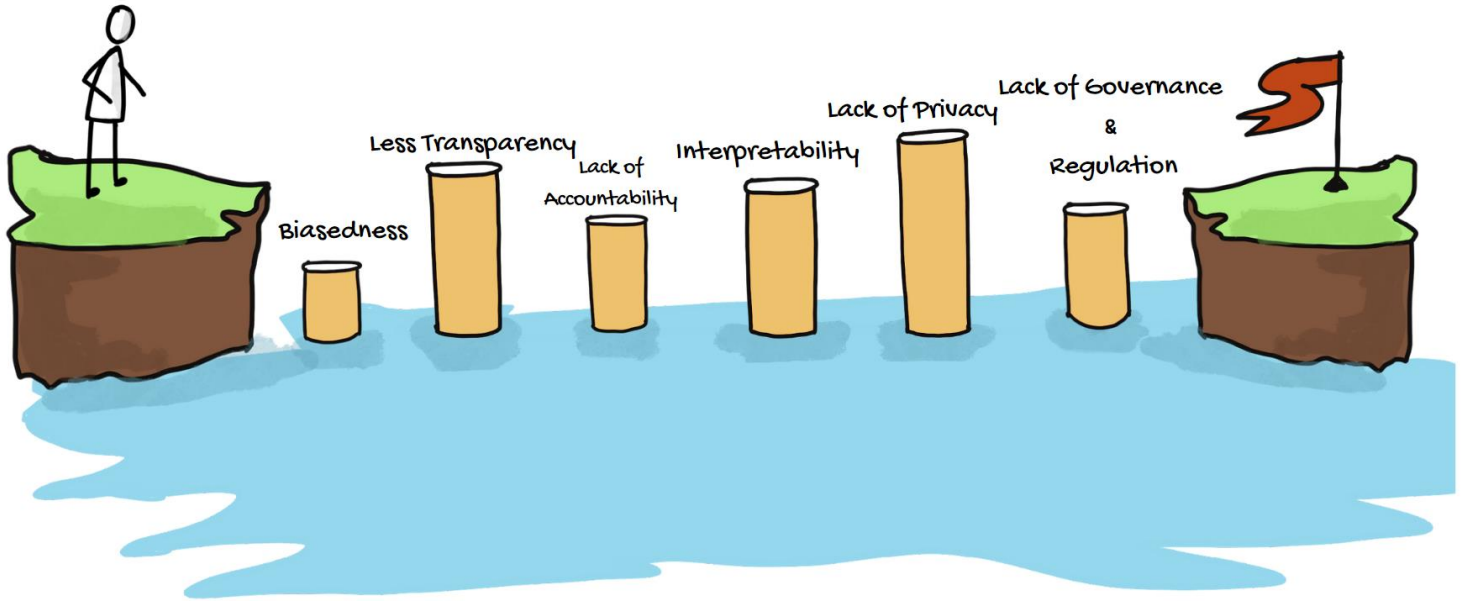
# What is Responsible AI

**What is Responsible AI?**

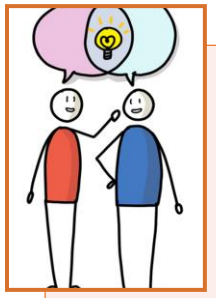



Responsible AI is a set of practices with focus to design, develop, and deploy AI applications in a safe, trustworthy and ethical manner.

**What are the challenges of Responsible AI?**



# Principles of Responsible AI - Microsoft

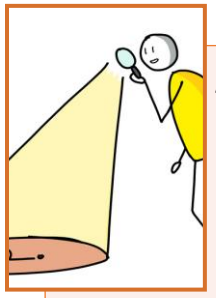


**Fairness**

- AI systems must treat everyone fairly

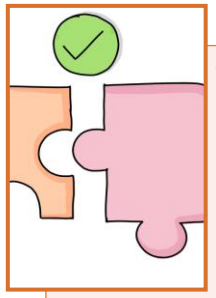
**Inclusiveness**

- AI systems must empower everyone and engage people



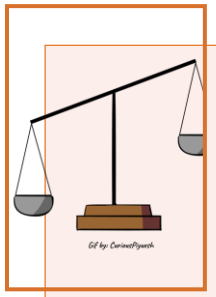
**Accountability**

- People must be accountable for AI systems



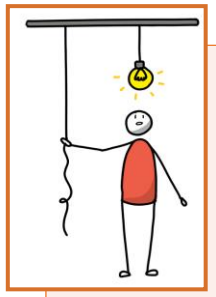
**Transparency**

- AI systems must be understandable and transparent



**Reliability & Safety**

- AI systems must perform reliably and safely



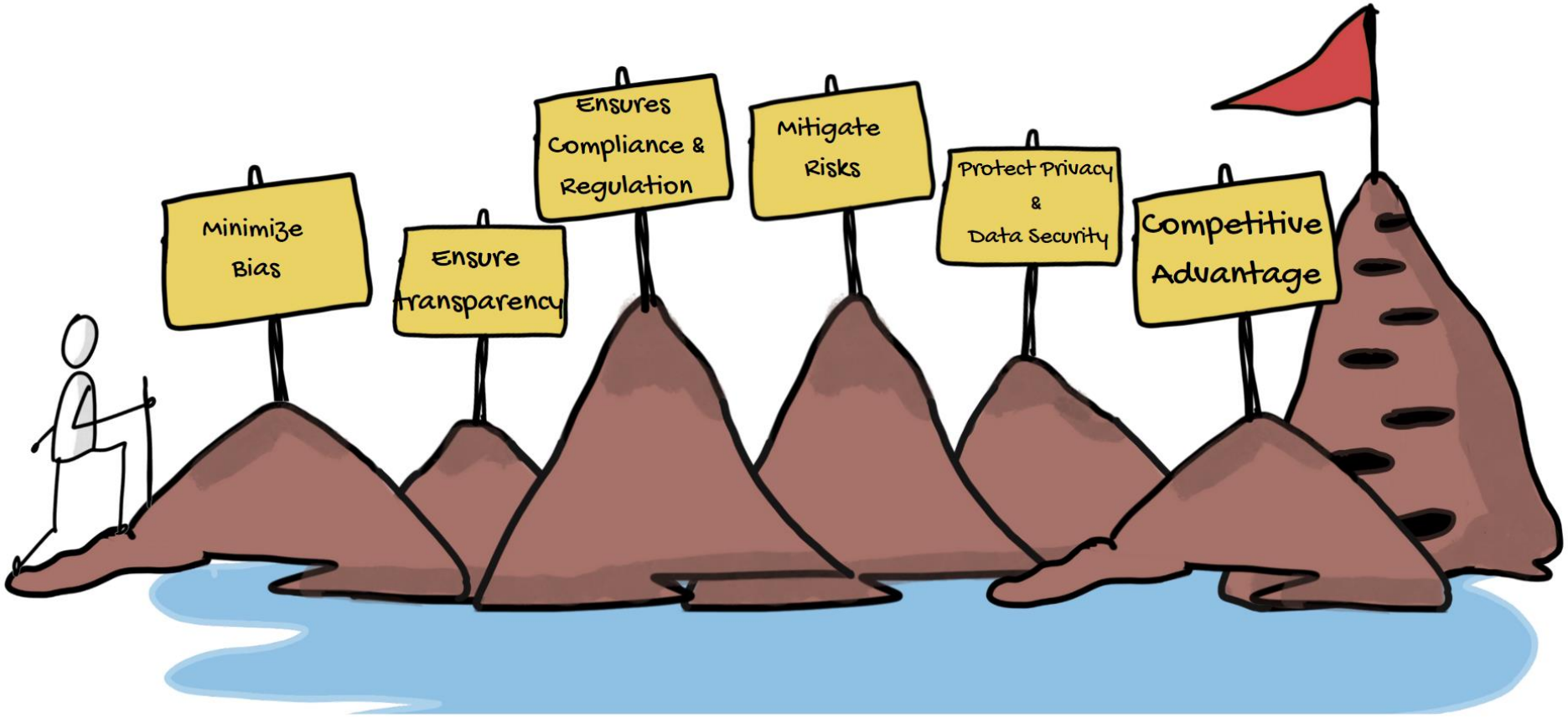
**Privacy & Security**

- AI systems must be secure and respect privacy

NSE talent sprint

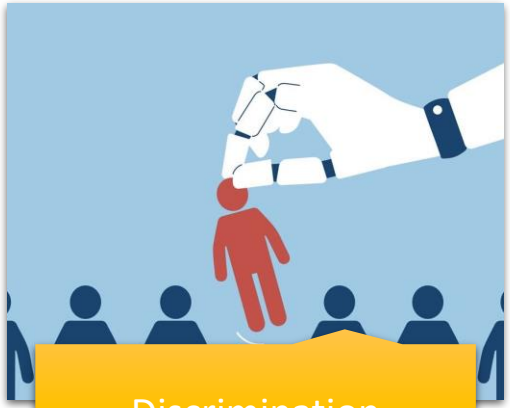
# Benefits of Responsible AI

**Why Responsible AI?**

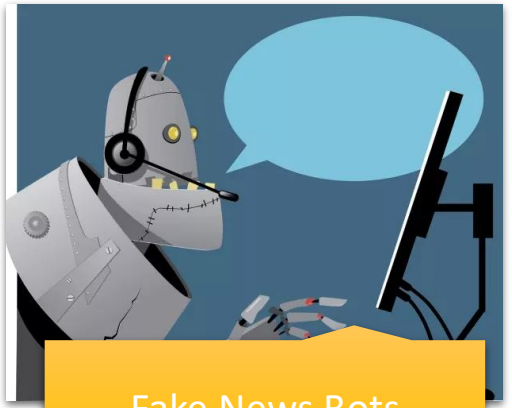


# Threats to Responsible AI

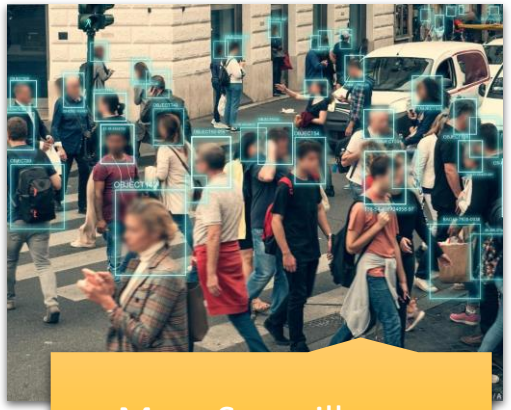
Deep Fakes



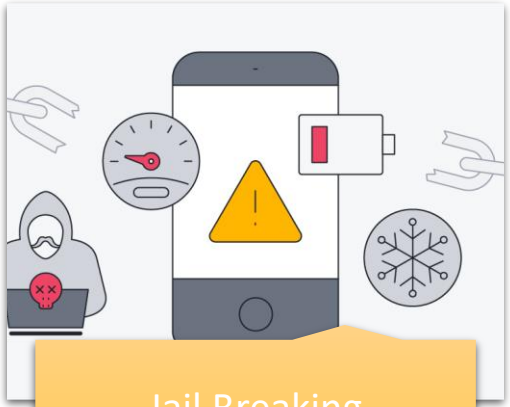
Discrimination



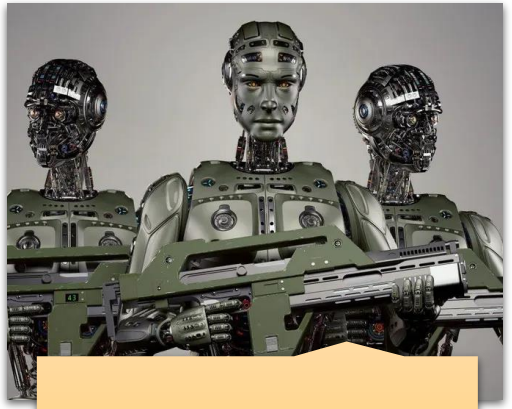
Fake News Bots



Mass Surveillance



Jail Breaking



Weapon Automization

# Vulnerabilities to LLM Models

- Direct Prompt Injection
- Indirect Prompt Injection

Prompt Injections

- Manipulate training data
- Improper filter
- Unrestricted data access
- Lack of data scrubbing

Data Leakage

- Hallucination
- Factually Incorrect data
- Illogical Outputs
- Source Mix
- Overindulgence

Overreliance

- URL strings
- Permit SQL raw query
- Chained Plugin – no distinct authorization
- User check-in for authorize

Insecure Plugins

- Continuous input overflow
- Repetitive long inputs
- Recursive context window
- Variable-input length flood

Denial of Service

# Prevention of LLM Models Vulnerabilities

## Prompt Injections

- Input verification
- Context-based filters
- Update & fine-tune LLM
- Monitor & log LLM interactions

## Data Leakage


- Data Sanitize
- Principle of Least Privilege
- User Policies
- User awareness

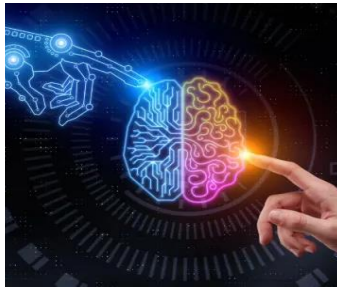
## Overreliance

- Continuous Monitoring
- Output Verify
- Divide Tasks
- Risk Communicate
- Secure Coding
- Safe UI & API

## Insecure Plugins

- Parameterized input
- Avoid chain plugin
- Least-privilege access control
- Robust authentication

## Denial of Service



- Cap Requests
- API rate limits
- Monitor LLM resource utilization
- Spread awareness

NSE talent sprint

Thank You!