GHULAM ISHAQ KHAN INSTITUTE
OF ENGINEERING SCIENCES AND TECHNOLOGY

AGENTIC AI

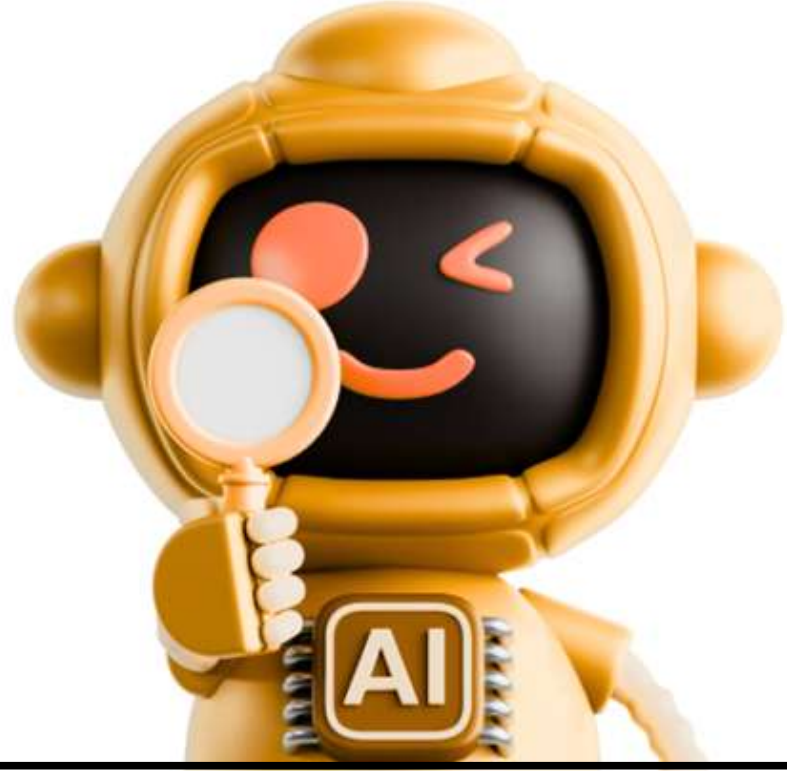
CS202 LECTURE 22

PRESENTOR
PROF DR S M HASAN ZAIDI
PRESIDENT'S PRIDE OF PERFORMANCE
PRO-RECTOR (ACADEMIC), GIKI

INTRODUCTION TO AGENTIC AI

Agentic AI:

Systems that **Act**, **Plan**, and **Pursue Goals Autonomously**



INTRODUCTION TO AGENTIC AI

Active Agents that

Collaborate with Humans,

Interact with Digital Environments, and

Execute Complex Workflows

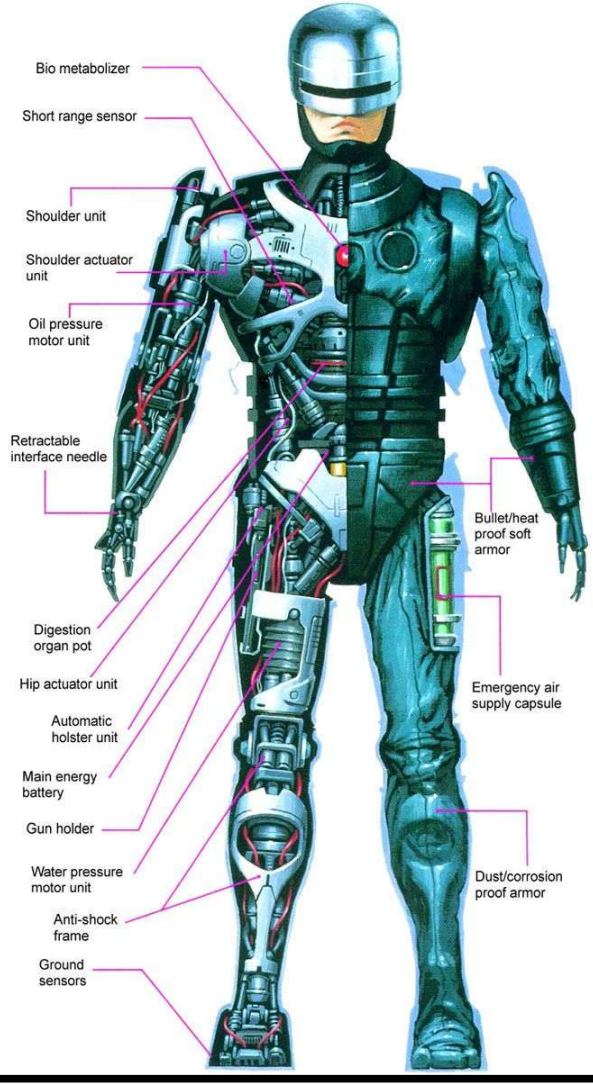
INTRODUCTION TO AGENTIC AI

In this Presentation, We Explore:

- **Scientific Foundations,**
- **Architecture,**
- **Capabilities,**
- **Applications,**
- **Challenges,**

and

- **Future Directions** of **Agentic AI**



WHAT IS AGENTIC AI?

Agentic AI Acts

Traditional AI Models Predict

WHAT IS AGENTIC AI?

Integrate

- **Decision-making,**
- **Planning,**
- **Reasoning,**

and

- **Actions**

within an **Environment**

WHAT IS AGENTIC AI?

Capable of

- **Breaking Down Tasks,**
- **Identifying Tools it Need,**
- **Using APIs or Software,**

and

- **Iteratively Improve Outputs**

WHAT IS AGENTIC AI?

Shift toward

AI Systems

Behaving More Like

Autonomous

Digital Workers

or **Collaborators**

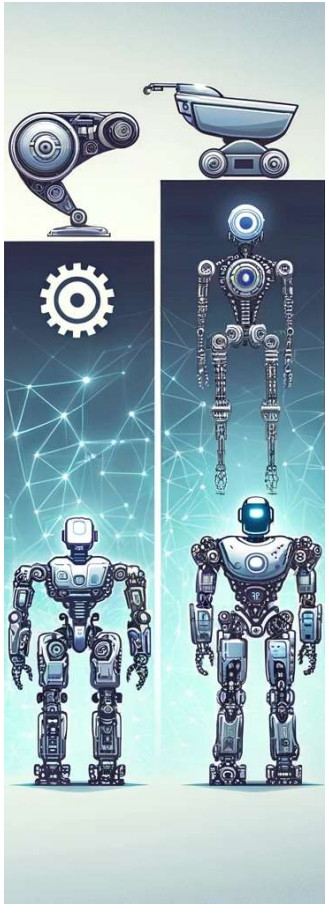
EVOLUTION TOWARD AGENCY

Classical AI (1980s and 1990s):

- Focused on **Symbolic Planning** and **Rule-based Agents**
- Systems had **Reasoning Abilities** But **Lacked Adaptability**

Deep Learning Revolution (2012–2020):

- **Emphasized Perception** (Vision, Speech, Pattern Recognition)
- **Lacked Agency**



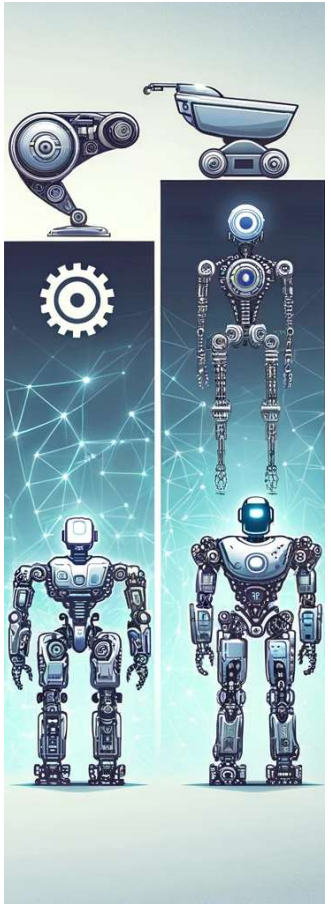
EVOLUTION TOWARD AGENCY

Emergence of Large Foundation Models and Transformers:

- Models Gained Generalizable **Reasoning** Abilities

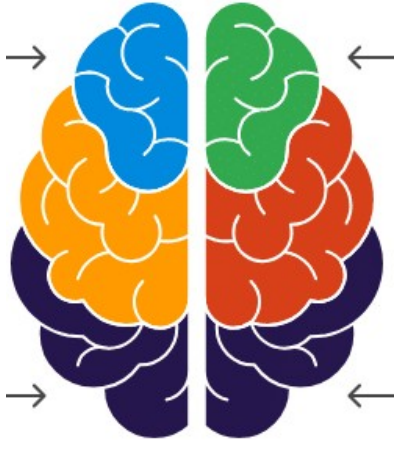
Agentic AI Represents the Next Stage:

- Combining the Reasoning Strength of Foundation Models with **Autonomous Planning**, **Tool Use**, and **Continuous Learning**
- Leading to AI Systems that **Perform Multi-Step Tasks** and **Drive Scientific Workflows**



CORE CAPABILITIES

- **Long-horizon Planning:** **Break down** complex goals into sequenced tasks
- **Tool Use:** Interacting with **Databases**, **APIs**, **Web Environments**, or **Computational Tools**
- **Memory:** **Maintaining Persistent State** across Sessions, Making them **Capable of Long-term Projects**

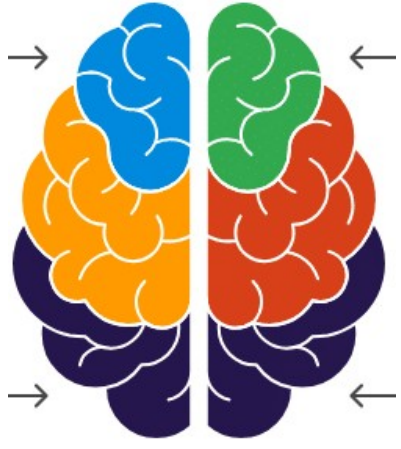


CORE CAPABILITIES

- **Self-Reflection:** **Evaluating its own outputs** and making corrections

- **Autonomous Workflow Execution:** Running **Experiments**, **Simulations**, or **Data-Processing** Pipelines End-To-End

- **Allow Agents to Operate Like:** **Autonomous Research Assistants** or **Digital Lab Technicians**



ARCHITECTURAL COMPONENTS

Agentic AI Architectures:

- **Modular**

and

- **Inspired by Cognitive Science**

ARCHITECTURAL COMPONENTS

- **Key Components:**
  - **Policy/Planner:** **Determines Actions** Based on **Goals** and **Environment States**
  - **World Models:** **Internal Simulators** Allowing Agents to **Predict Outcomes** of Actions

ARCHITECTURAL COMPONENTS

- **Key Components:**
  - **Memory Systems:** May Include **Short-term Working Memory** and **Long-term Knowledge Storage**
  - **Feedback Loops:** Enable **Iterative Refinement** i.e., Agent **Checks**, **Corrects**, and **Optimizes** its Outputs
- A **Closed Loop** where AI can **Observe**, **Reason**, **Act**, and **Learn Continuously**

AGENT FRAMEWORK TYPES

- **Reactive Agents:** **Respond Immediately** to Stimuli **Without Planning**; Useful in **Robotics and Control**

- **Deliberative Agents:** **Build** Internal Models, **Plan** Ahead, and **Evaluate** Multiple Scenarios

- **Hybrid Agents:** **Combine Reactive and Deliberative Behaviors** for Robust Performance

AGENT FRAMEWORK TYPES

- **Multi-Agent Systems:** **Multiple Autonomous Agents** Collaborate or Compete to **Solve Distributed Problems**

- **Hierarchical Agents:** Higher-Level Agents **Oversee Lower-Level Agents**, Enabling **Scalability** for Large Tasks

- **Allow Agentic AI to Adapt** to **Specific Scientific or Engineering Contexts**

SCIENTIFIC APPLICATIONS OF AGENTIC AI

- **Automated Experiment Design:** Agents **Propose Hypotheses**, **Run Simulations**, **Analyze Results**, and **Refine Parameters**

- **Robot-Controlled Laboratories:** Agents **Orchestrate Robotic Equipment** for **High-Throughput Experimentation**

- **Scientific Discovery Engines:** Agents **Search Literature**, **Extract Concepts**, and **Form New Research Directions**

SCIENTIFIC APPLICATIONS OF AGENTIC AI

- **Multi-Scale Simulation Orchestration: Coordinate Complex Simulations** from Atomic to Macro Scale

- **Optimization and Control:** Intelligent Agents **Optimize Materials, Chemicals, Reactors, Network Systems**, etc.

- **Shift of Scientific Workflow** from Human-Driven to **Human-Supervised, Agent-Accelerated Research**

TOOLS & AUTONOMY IN PRACTICE

- Real-World Agentic Systems **Interact with Digital Infrastructure to Complete Tasks End-To-End**

- **Calling APIs, Querying Databases, or Interacting with Cloud Systems** to **Gather Information** or **Perform Computations**

- **Code-Generation Agents: Write, Test, and Execute Programs Autonomously**

TOOLS & AUTONOMY IN PRACTICE

- **Self-Debugging Workflows:** Agent **Identifies Errors, Revises Approaches, and Reruns Tasks**

- **Safety Protocols** Ensure **Agents Remain within Authorized Boundaries** and **Avoid Harmful Actions**

- This **Tool-using Capability** makes Agentic AI **Extremely Powerful for Data-Intensive Sciences**

CHALLENGES IN AGENTIC AI

- **Reliability and Alignment:** Ensuring Agents **Interpret Goals Correctly** and **Behave Safely**
- **Control-Autonomy Trade-Off:** **More Autonomy** Increases both **Power and Risk**
- **Safe Tool Access:** Agents Interacting with Systems must **Follow Strict Boundaries**
- **Uncertainty Handling:** **Planning** becomes Difficult under **Unpredictable Environments**
- **Evaluation Complexity:** **Emergent Behaviors** from Interacting Components make **Evaluation Non-Trivial**

ETHICAL & SOCIETAL CONSIDERATIONS

- With **Autonomy** Comes Increased **Ethical Responsibility**
- **Accountability:** Who is **Responsible** for Autonomous Actions?
- **Verifiability:** Can we **Audit** and Explain an Agent's Decisions?
- **Human Oversight:** How do we Maintain **Control** without Limiting Capabilities?
- **Risk of Unintended Behavior:** Agents may **Adapt or Discover** Solutions Outside the Intended Scope
- **Hence,** Establishing **Governance** Frameworks, Standardized **Auditing**, and Transparent **Documentation** is Essential

FUTURE DIRECTIONS

- **Future of Agentic AI:** Deeply Intertwined with **Scientific Progress**
- **General-Purpose Scientific Agents** Capable of **Forming Hypotheses** and **Designing Experiments**
- **Multimodal Agents** Integrating **Text, Vision, Simulations, Lab Equipment, and Robotics**
- **Artificial Scientists** that Autonomously **Explore Scientific Spaces** and **Make Discoveries**

FUTURE DIRECTIONS

- **Cognitive Architectures** Combining **Memory, Perception, Reasoning, and Action**
- **Safe Self-Improving Agents** Capable of **Refining their Abilities** under Constrained Supervision
- These Developments could **Accelerate Scientific Discovery** by Orders of Magnitude

CONCLUSION

- **Significant Leap** from **Predictive Modeling** to **Autonomous Problem-Solving**
- **Potential Impact** Spans **Drug Discovery, Materials Design, Engineering Optimization, Climate Modeling, Robotics,** and beyond
- **Key Challenge** is to Harness this Power Responsibly, **Balancing Autonomy with Safety and Oversight**
- **Scientists and Researchers** stand at the **Frontier of Redefining Experimentation, Discovery, and Knowledge Creation** with Agentic Systems

THANK YOU !