4. Real-World Applications and Future Trends

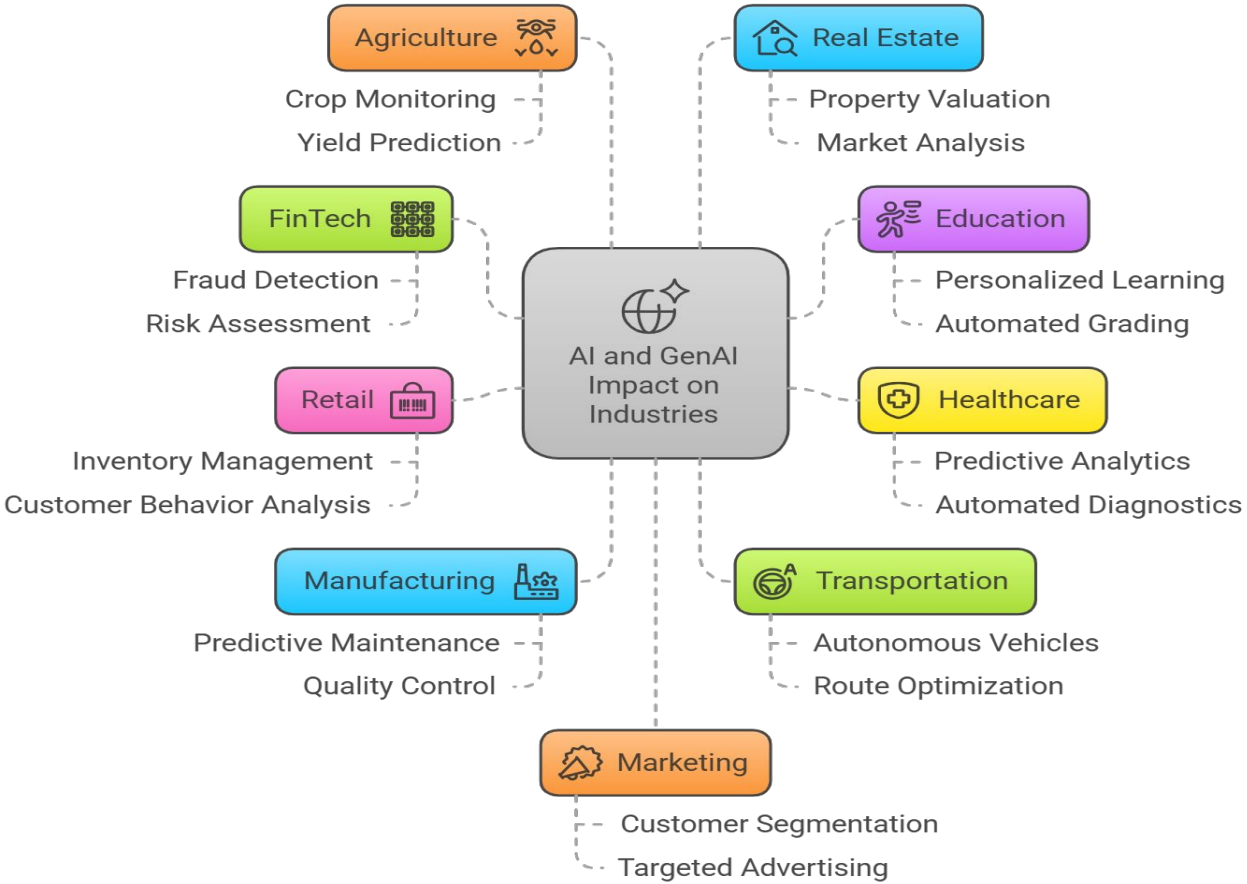
Exploring AI Applications, Security and Trends

CAZE LABS
ignite innovations, harness open source!

www.cazelabs.com

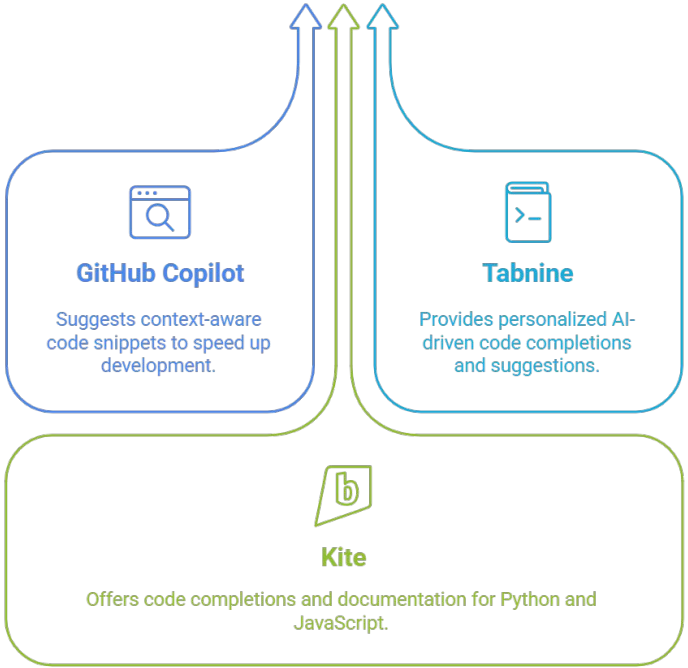
Use Cases of AI Copilots

Applications of AI Copilots



Unlimited Opportunities!

Examples : Software Development



https://github.com/features/copilot

https://www.tabnine.com/

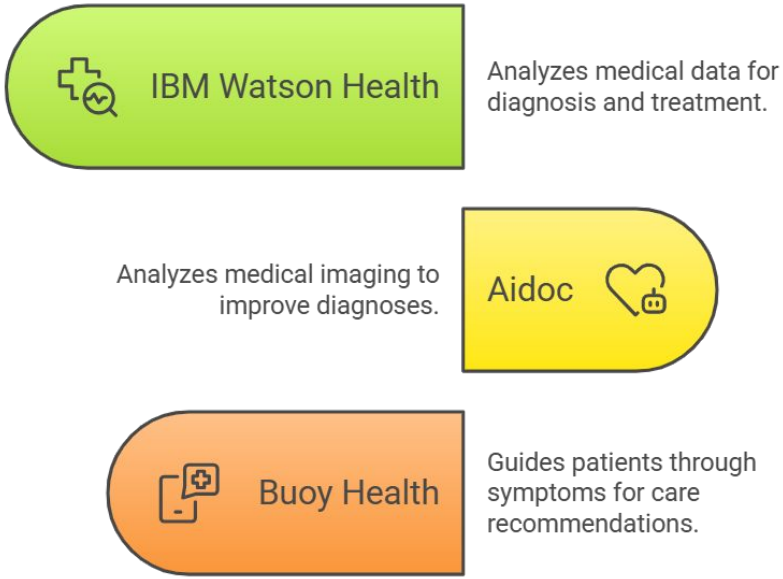
https://open-vsx.org/extension/kiteco/kite

These are just samples. There are so many!

We are working:

- Security Reviewer and Patching

Examples : Healthcare



https://www.ibm.com/industries/healthcare

https://www.aidoc.com/

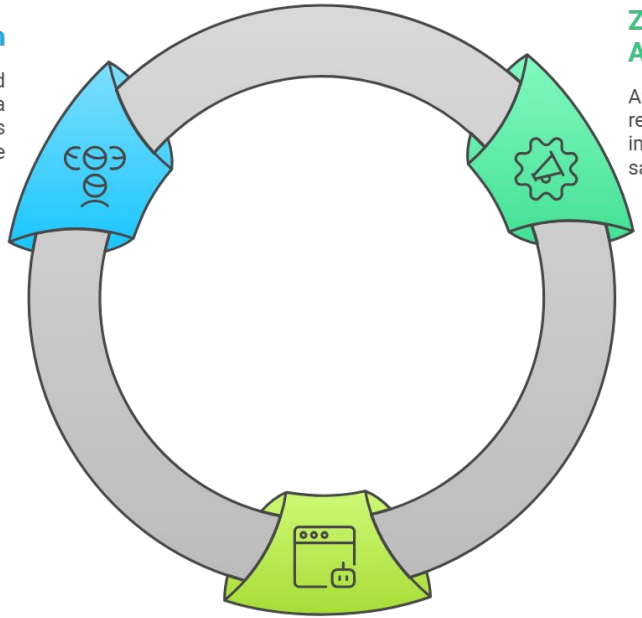
https://www.buoyhealth.com/

These are just samples. There are so many!

We are working:

- Medical Treatment Procedure Assistant

Examples : Customer Service



LivePerson

Combines AI and human agents for a seamless experience

Zendesk Answer Bot

Automates responses to FAQs, improving satisfaction

Ada

Provides AI-driven 24/7 support, resolving issues independently

https://www.liveperson.com/

https://www.zendesk.com/

https://www.ada.cx/

These are just samples. There are so many!

We are working:

- BizConAI – Automated business connections

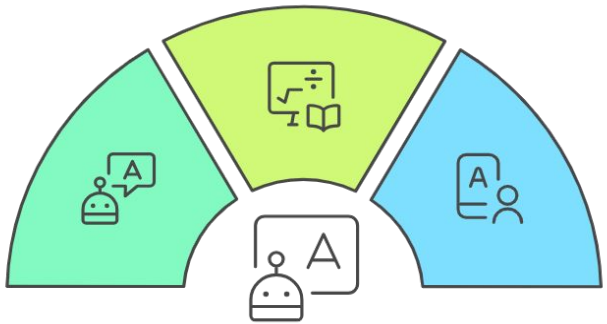
Examples : Education

Knewton Alta

An adaptive platform personalizing content based on student performance.

Socratic by Google

An AI app aiding homework by providing explanations and resources.



Duolingo

AI personalizing language learning by adapting to user progress.

https://www.wiley.com/en-us/education/alta

https://socratic.org/

https://www.duolingo.com/

These are just samples. There are so many!

We are working:

- Data Sense : Making sense from scattered data.
- Do you have any use case for us?

AI Security

- Lets understand the pitfalls

Scope

- AI Security Challenges
- Meeting the challenges -The pointers
- AI Security Trends

AI is critical; But..!

The global AI software market is expected to grow from $136.55 billion in 2023 to **$1,811.77 billion by 2028**, at a CAGR of 53.68%

70% of organizations have experienced an AI-related security incident in the past year

The average cost of an AI security breach is **$3.86 million**

60% of organizations lack a AI security strategy comprehensive

85% of organizations believe that AI security is a top priority

Inherent risks imposed by AI!

- Increasing complexity of AI Models
- Rapid adoption across various industries
- Growing sophistication of cyber threats

AI Security Challenges

Core vulnerabilities: Software, hardware, data, and model integrity.

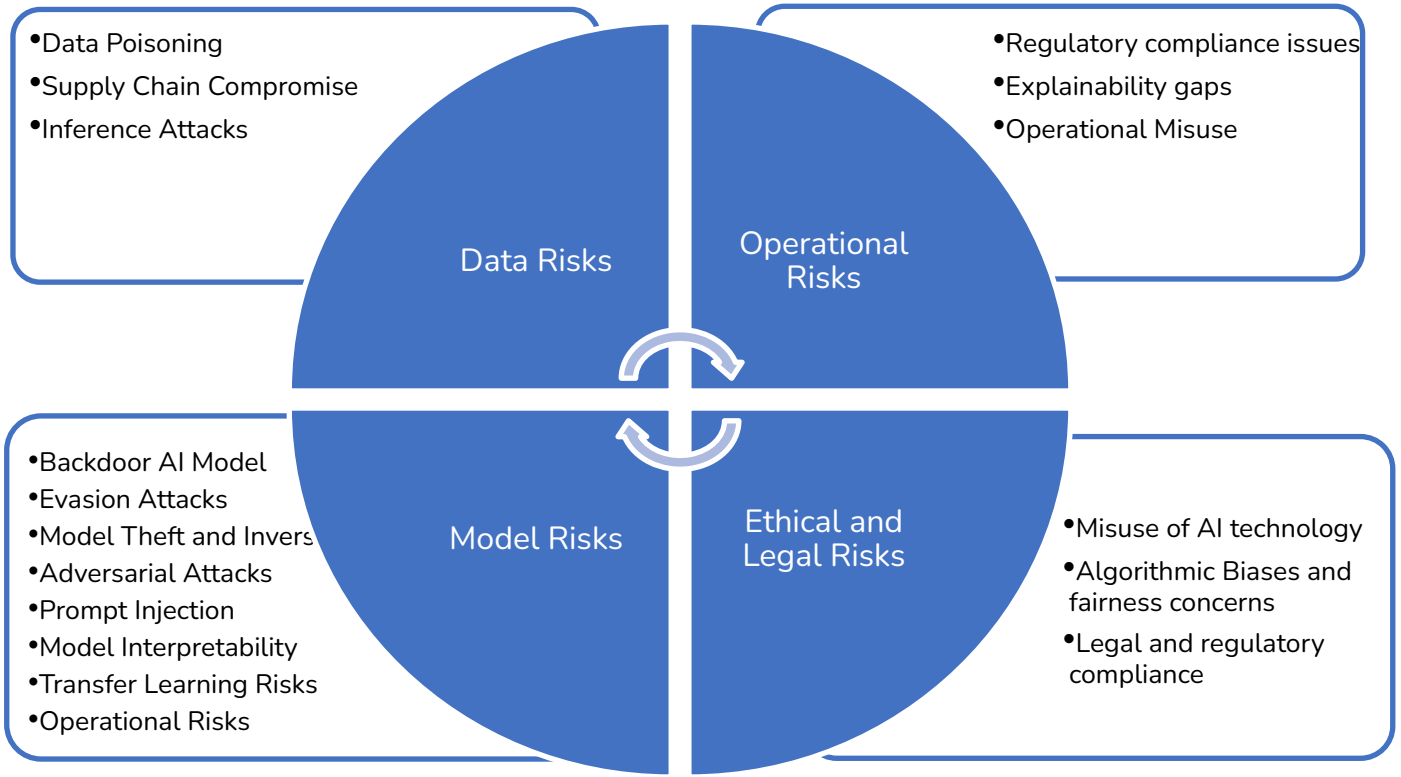
Emerging risks: Adversarial attacks, Data Poisoning, supply chain threats.

AI systems face complex threat landscape

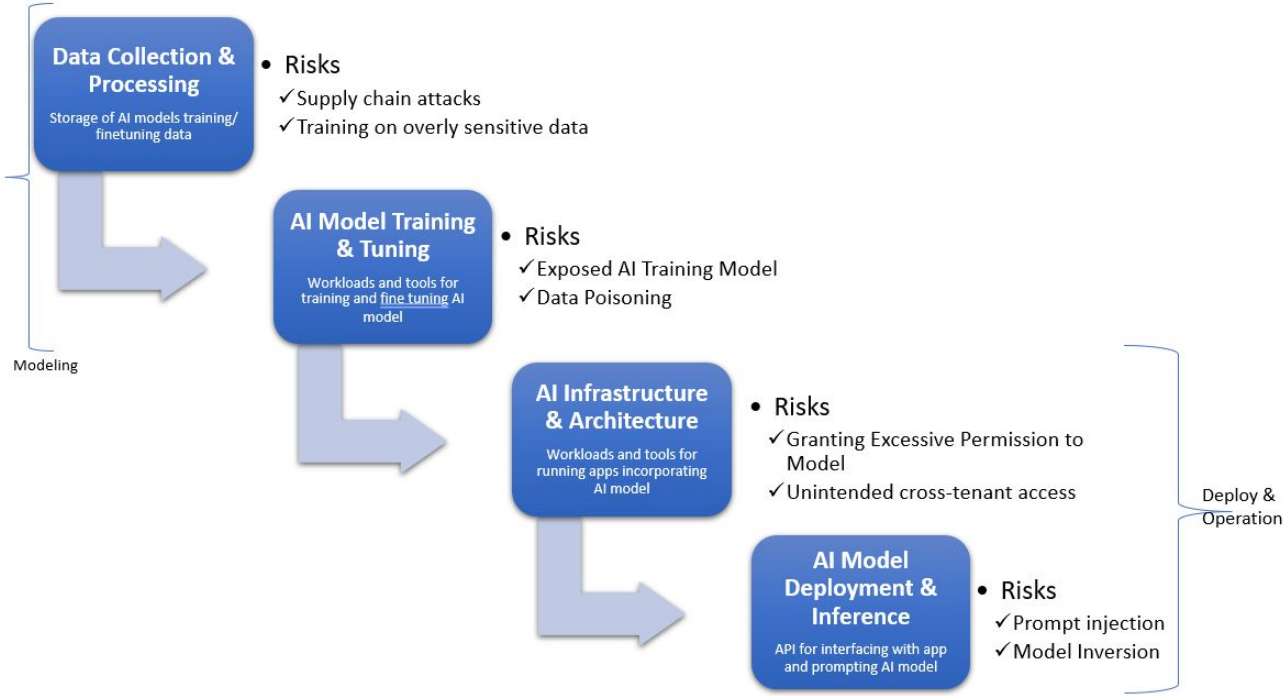
Impact: Compromised accuracy, reliability, and overall system security.

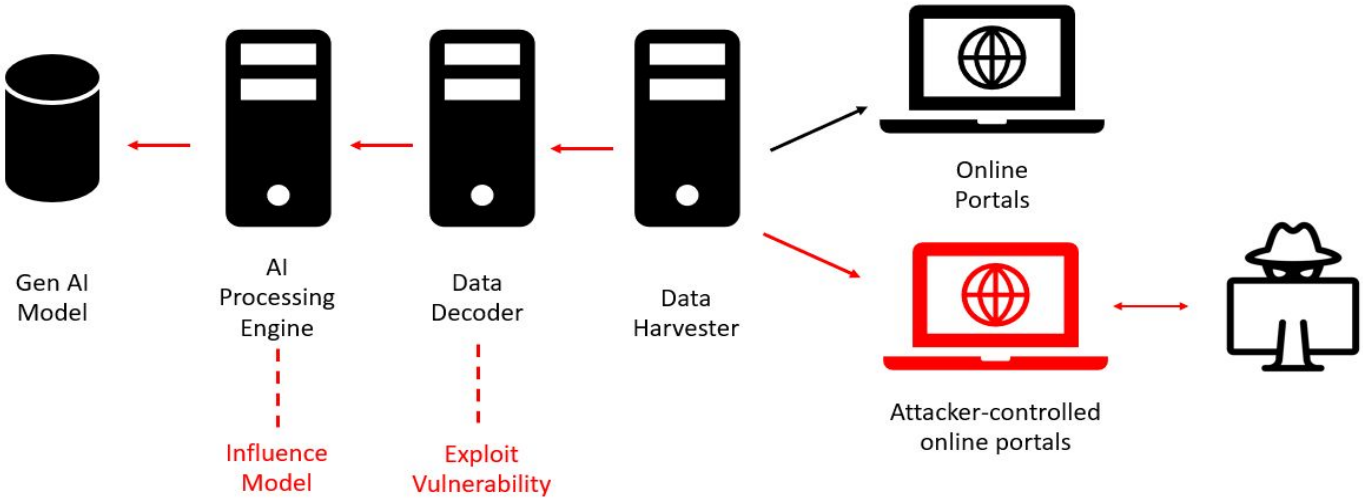
multifaceted approach is needed to handle!

The AI RISK Landscape



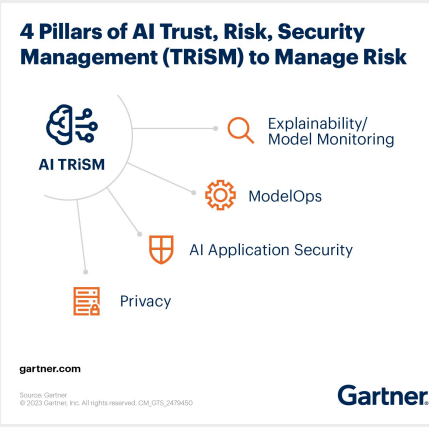
Security RISKs in AI pipeline

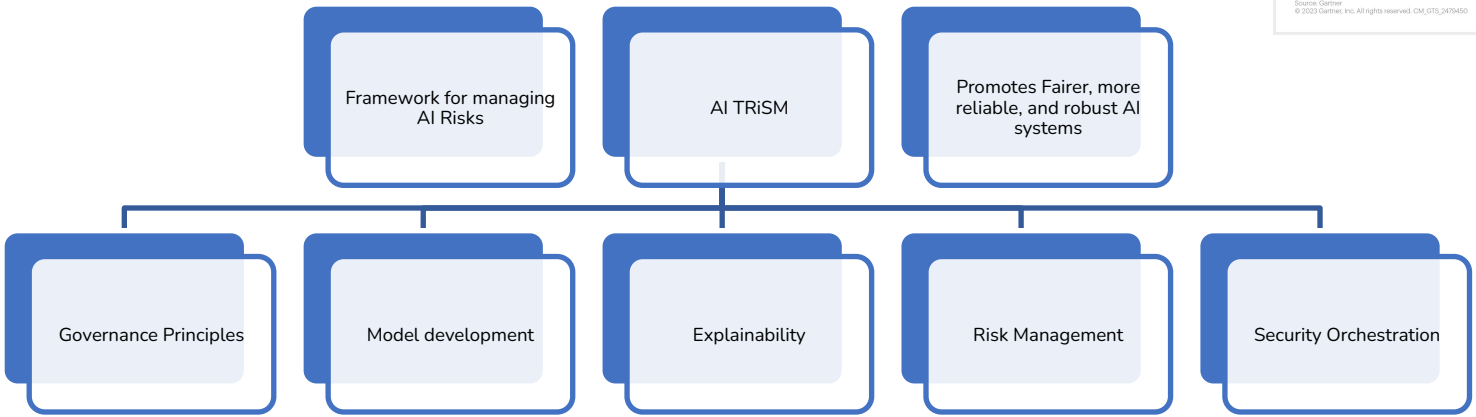




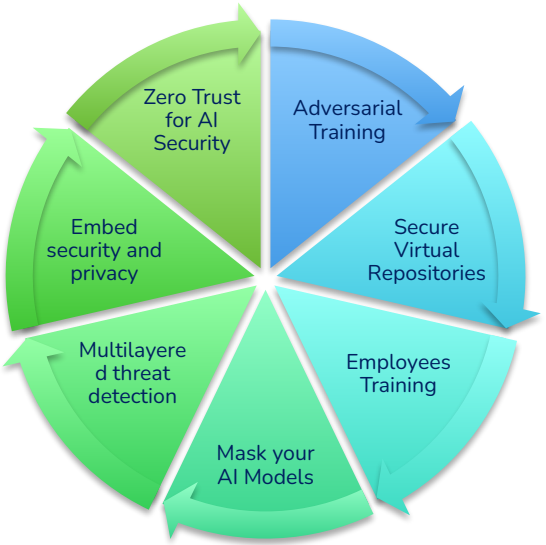
AI Model exploitation

AI TRiSM


4 Pillars of AI Trust, Risk, Security Management (TRiSM) to Manage Risk
AI TRiSM
Explainability/ Model Monitoring
ModelOps
AI Application Security
Privacy
gartner.com
Gartner


Framework for managing AI Risks
AI TRiSM
Promotes Fairer, more reliable, and robust AI systems
Governance Principles
Model development
Explainability
Risk Management
Security Orchestration

Good News! There are ways to ensure AI security!



Strategies for AI system protection

- Meta Neural Analysis
- Federated Learning
- Homomorphic Encryption
- Secure Multi-Party Computation

Advanced AI Security techniques

Comprehensive Security Measures for AI Systems

- Data Anonymization
- Threat Modeling
- Robust Access controls-RBAC,MFA
- Encryption
- Protect AI data in transit
- Adversarial Training
- Secure Coding
- Model watermarking
- Hardening hardware
- Bias Mitigation - Bias Detection Tools, Diverse Datasets
- Anomaly detection for model monitoring
- Regular Security Audits and Penetration Testing
- Monitoring and Logging, Incident Response
- Legal and Ethical Guidelines
- Employee Training and Awareness
- stay up-to-date

AI Security Frameworks and Standards

- NIST AI Risk Management Framework
- MITRE Sensible Regulatory framework
- EU AI ACT
- OWASP TOP 10 for LLM's
- Google Secure AI framework
- GDPR

- Enhanced Security
- Improved decision-making
- Regulatory Compliance
- Operational resilience
- Increased trust and transparency

companies that take pre-trained machine learning models from public repositories like HuggingFace or TensorFlow Hub are at risk of bringing cyber threats

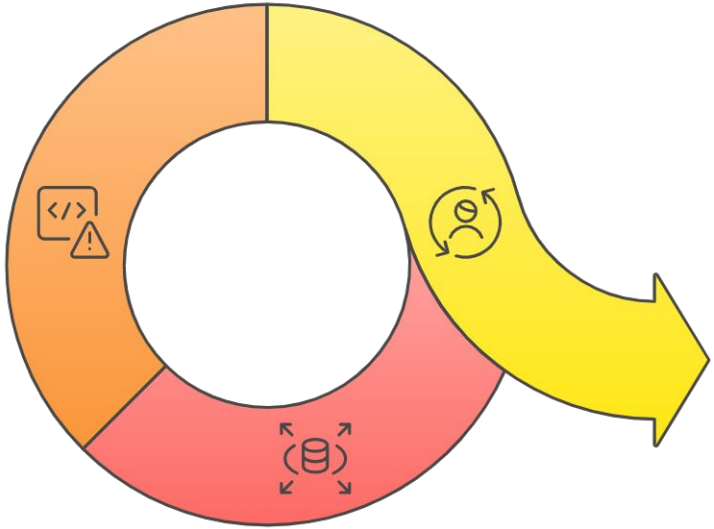
The Future of AI Security

Challenges and Ethical Considerations

Bias, privacy, and accountability in Agentic AI

BIAS

- produce systematically prejudiced results
- biased data



1

Data Bias

Historical data reflects societal biases, leading to skewed AI learning.

2

Algorithmic Bias

Algorithms designed without diverse perspectives introduce bias.

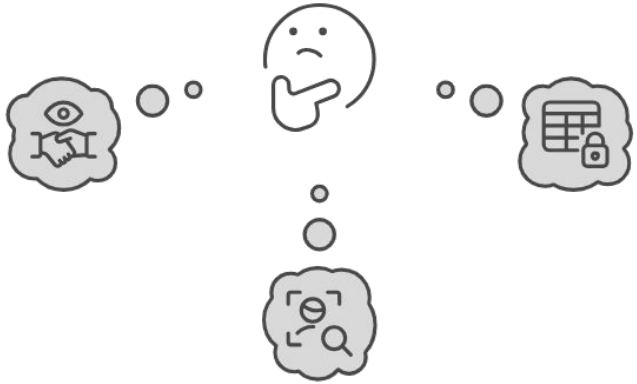
3

Feedback Loops

User interactions reinforce existing biases, worsening the problem.

Privacy

- collection, storage, and processing of sensitive information
- rely on vast amounts of personal data



Informed Consent

Ensures users are aware of data usage and agree to it, fostering trust.

Data Security

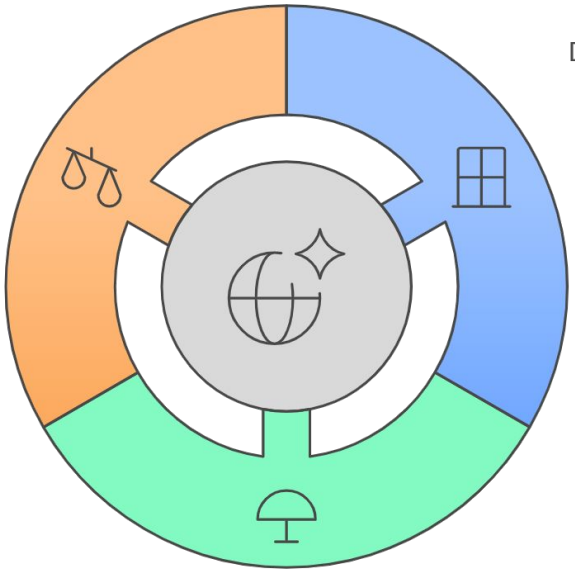
Protects personal data from breaches, maintaining trust in AI systems.

Surveillance Ethics

Balances security needs with individual privacy rights, addressing ethical dilemmas.

Accountability

- the responsibility of developers, organizations, and users for the outcomes produced by AI systems
- Hard to identify who is accountable for decisions made



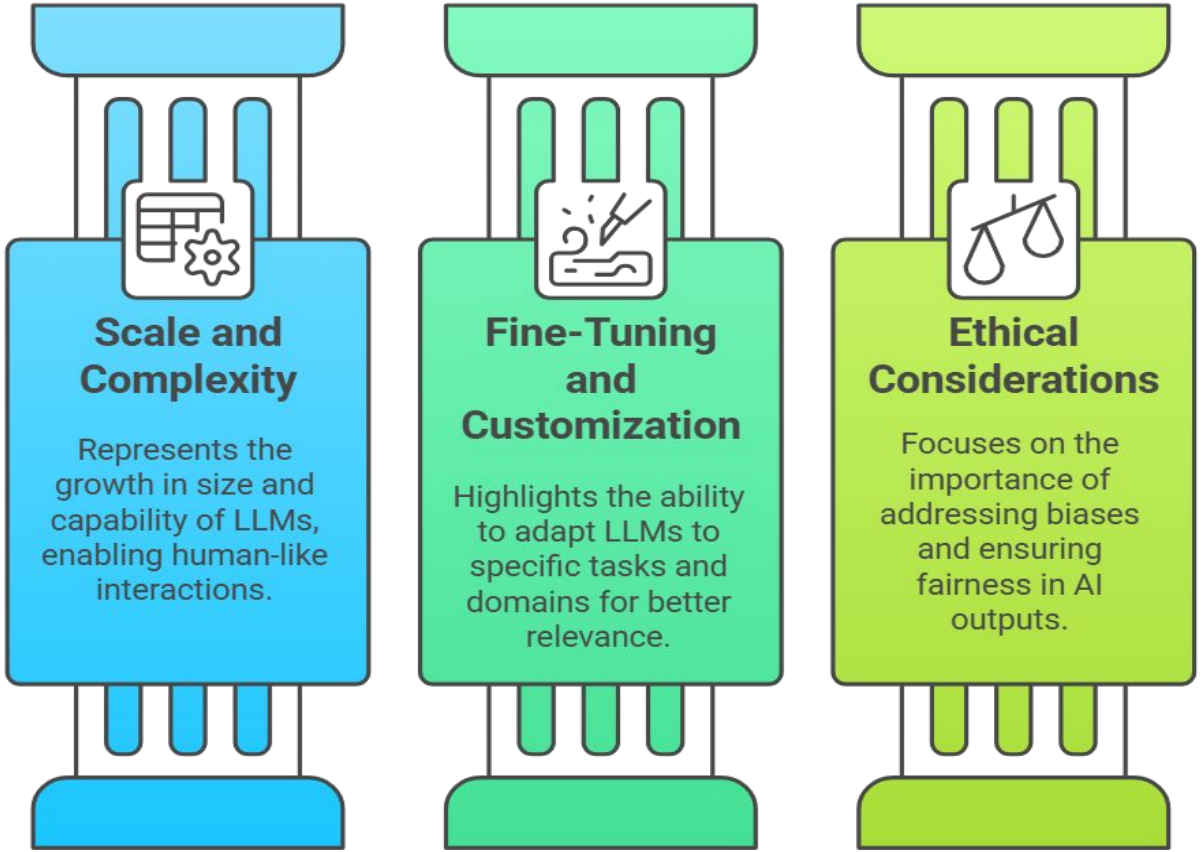
Future Trends

Dynamic, Unpredictable....!

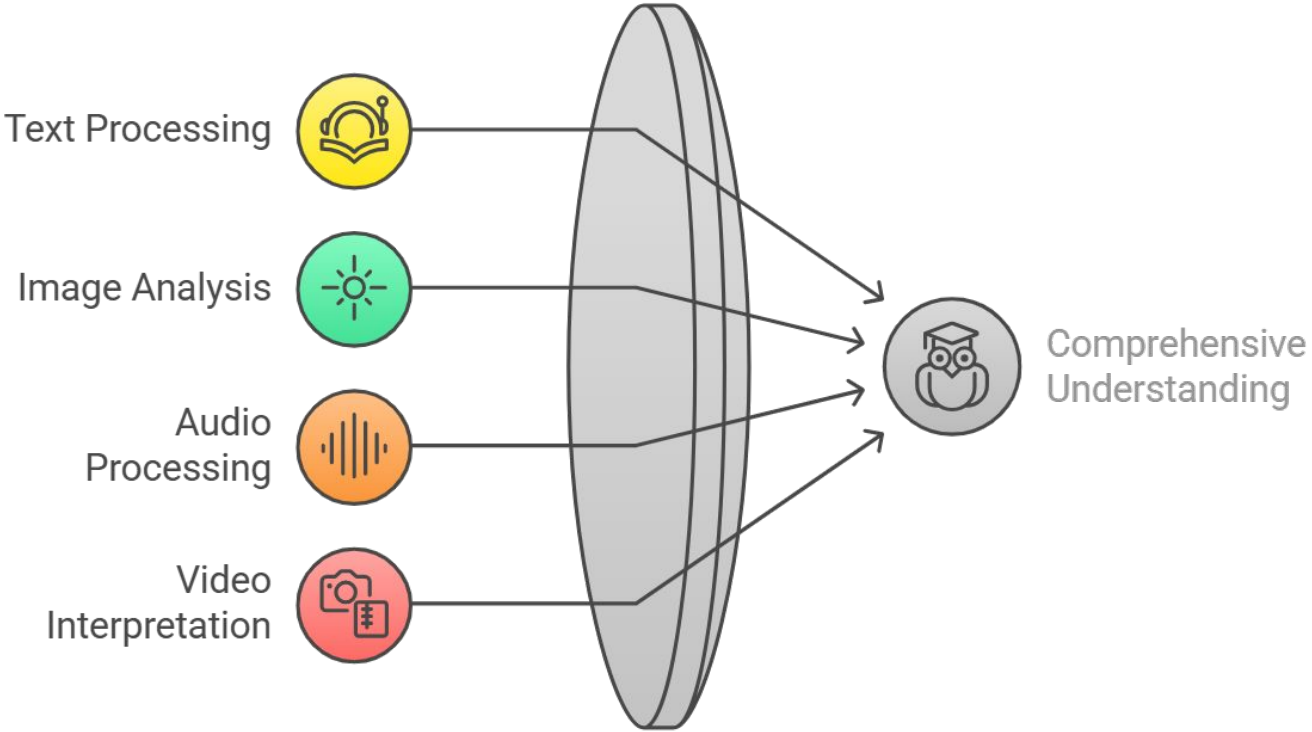
Scope

- Advances in LLMs and multimodal AI.
- The role of AI Copilots in shaping the future of work

LLMs are getting better!



Multimodal


Text Processing
Image Analysis
Audio Processing
Video Interpretation
Comprehensive Understanding

Agentic AI

Agentic AI refers to artificial intelligence systems designed to operate with a degree of autonomy, enabling them to make decisions and perform tasks without continuous human intervention.

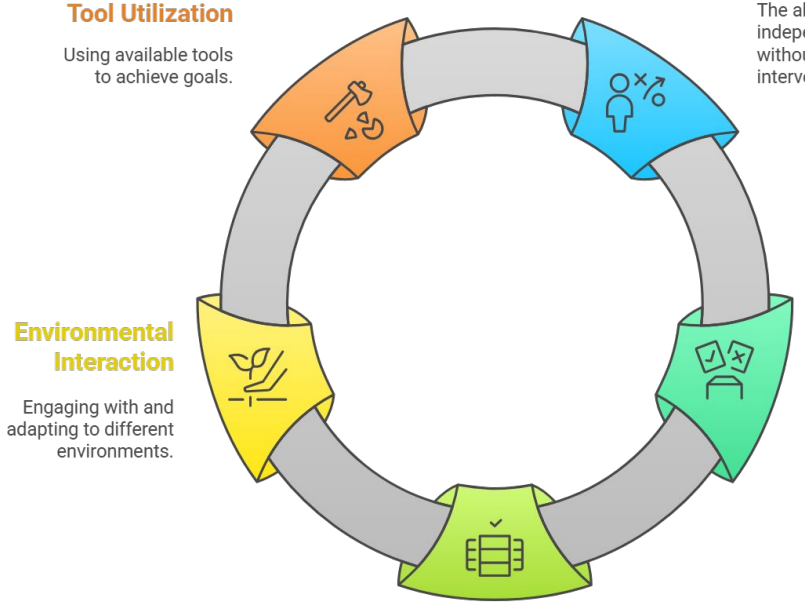
Agentic AI

Enables autonomous decision-making

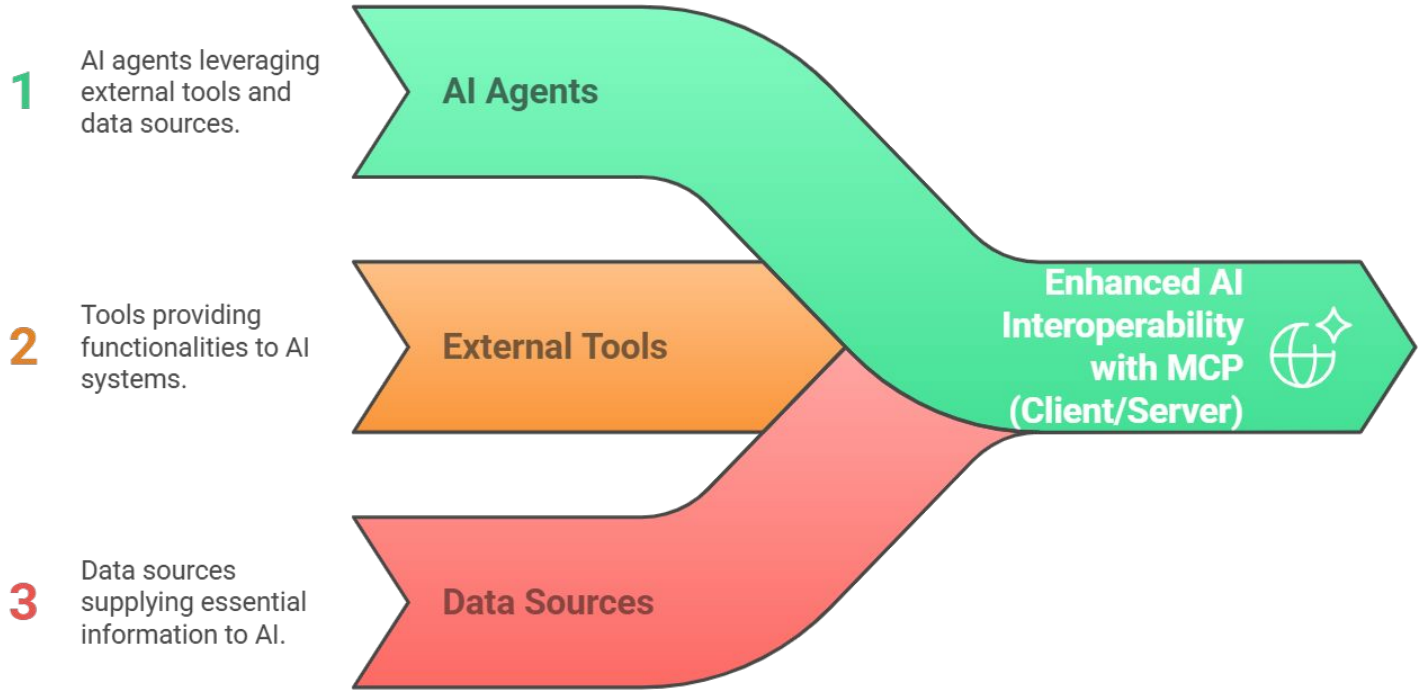
VS

Traditional AI

Requires explicit instructions



Model Context Protocol (MCP)



AI Copilots – becoming part of our daily life..?!

Automation of Repetitive Tasks

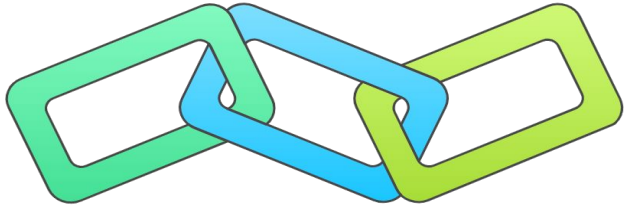
Streamlines routine tasks to enhance focus on strategic activities

Real-Time Assistance

Provides immediate support to streamline workflows and reduce errors

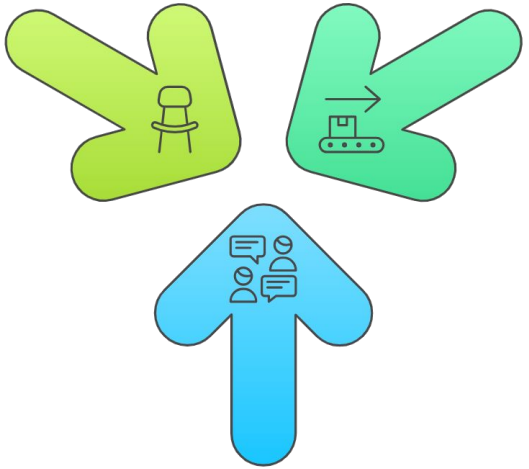
Data Analysis and Insights

Analyzes data to extract actionable insights for informed decision-making



Personalized Experiences

AI adapts to individual preferences for efficiency.



Streamlined Processes

AI optimizes workflows by automating tasks and providing suggestions.

Improved Collaboration

AI facilitates communication and task organization.

Knowledge Enhancement

Provides access to vast knowledge bases.

Creative Support

Assists with creative tasks and collaboration.

Skill Enhancement

Offers real-time feedback for skill improvement.

5. Resources and Pointers

Links to tutorials, documentation, and research papers.

Recommended tools and platforms for building AI Copilots.

Links to tutorials, documentation, and research papers

1. GeeksforGeeks: 7 Steps to Learn AI From Scratch in 2024
2. GeeksforGeeks: 10 Must Read Machine Learning Research Papers
3. TechRepublic: The 10 Best AI Courses That Are Worth Taking
4. GeeksforGeeks: Top 10 AI Tools for Creating Research Papers
5. GitHub: Must Read Papers for Data Science, ML, and DL
6. Academia Insider: The Best AI Tools for Research Papers and Academic Research
7. Tech.co: 20 Best Free AI Training Courses for 2024
8. GitHub: Awesome AI Tutorials and Surveys
9. Texta: The Ultimate Guide to Starting Your AI and Machine Learning Journey
10. PhDTalks: Machine Learning Research Papers for Beginners in 2025

Recommended tools and platforms for building AI Copilots

Tool/Platform	Description	Link
Hugging Face Transformers	Open-source platform for building AI models, including conversational copilots.	Visit Site
LangChain	Open-source framework for building AI copilots using large language models (LLMs) and custom workflows.	Visit Site
LlamaIndex (GPT Index)	Open-source tool for building AI copilots with data integration and natural language search.	Visit Site
OpenAI API (Free Tier)	While OpenAI is not fully open-source, it offers a free tier to experiment with AI copilots.	Visit Site
FastChat (By LMSYS)	Open-source platform to build and deploy chatbots and AI copilots with support for LLaMA and OpenAI APIs.	Visit Site
Rasa	Open-source conversational AI platform for building AI copilots with customizable UI components.	Visit Site
ChromaDB	Open-source AI-native database for building context-aware copilots and AI assistants.	Visit Site
Haystack (deepset.ai)	Open-source framework for building production-ready, UI-integrated AI copilots for search and Q&A.	Visit Site
Auto-GPT	Open-source experimental AI agent that automates complex tasks using LLMs like GPT-4.	Visit Site
Chatbot UI	Open-source chat UI framework for building AI copilots with support for OpenAI and open models.	Visit Site

Thank You!

www.cazelabs.com