Arxiv Papers::

1. **MCP Safety Audit: LLMs with the Model Context Protocol Allow Major Security Exploits**

Description: This paper discusses the security risks associated with the Model Context Protocol (MCP) for LLMs, highlighting vulnerabilities and introducing a safety auditing tool, MCPSafetyScanner, for assessing MCP server safety.

Link: Read the paper

2. **UMC: A Unified Bandwidth-efficient and Multi-resolution based Collaborative Perception Framework**

Description: The paper proposes a unified collaborative perception framework named UMC, aimed at optimizing communication, collaboration, and reconstruction processes in multi-agent collaborative perception tasks.

Link: Read the paper

3. **Autono: A ReAct-Based Highly Robust Autonomous Agent Framework**

Description: This work presents a robust autonomous agent framework that dynamically generates actions based on prior trajectories and implements a multi-agent collaboration mechanism, enhancing adaptability and efficiency.

Link: Read the paper

4. **Large Language Model Enhanced Multi-Agent Systems for 6G Communications**

Description: The paper discusses a multi-agent system designed to enhance communication tasks in 6G using large language models, focusing on aspects like data retrieval and collaborative planning.

Link: Read the paper

5. **Reinforcement Learning for Bidding Strategy Optimization in Day-Ahead Energy Market**

Description: This research focuses on developing a bidding strategy for sellers in energy markets using reinforcement learning, optimizing bidding processes through learned historical data.

Link: Read the paper