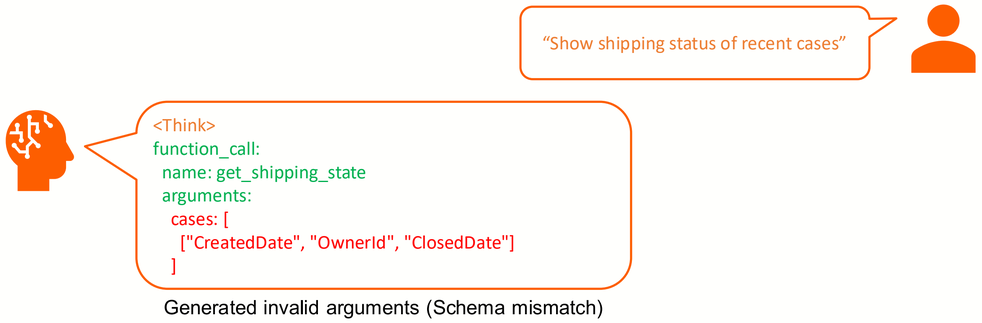
Author: วิจักขณ์ มะโนปราง **Email**: wijak.mano@gmail.com **Tel:** 095-431-2751 **Advisor:** ดร.วราสิณี ฉายแสงมงคล

Agentic tools with Model Context Protocol (MCP) for CRM Actions

Abstract

การนำโมเดลภาษาขนาดใหญ่ (LLM) มาใช้งานเป็น AI Agent ในระบบบริหารความสัมพันธ์ลูกค้า (CRM) ยังคงประสบปัญหาด้าน**ความซับซ้อนของการเชื่อมต่อเครื่องมือ** ความ**ไม่เป็นมาตรฐานของ API** และความ**ผิดพลาดในการเรียกใช้งานเครื่องมือ**โดยอัตโนมัติ

โครงงานนี้นำเสนอ **Agentic CRM Copilot** ที่เชื่อมต่อ LLM กับเครื่องมือ CRM ผ่าน **Model Context Protocol (MCP)** เพื่อสร้างมาตรฐานกลางในการนิยามเครื่องมือ การตรวจสอบพารามิเตอร์ และการควบคุมการเรียกใช้งานอย่างเป็นระบบ พร้อมออกแบบโครงสร้างการควบคุมการทำงานของ Agent แบบ **Graph-Based Control (LangGraph)** เพื่อเพิ่มความเสถียรและความสามารถในการจัดการข้อผิดพลาดในการทำงาน



Generated invalid arguments (Schema mismatch)

Problem

จากงานวิจัย **CRMArena (Salesforce AI Research 2025)** ซึ่งจำลองสภาพแวดล้อมการทำงานของระบบ CRM จริง พบว่าแม้ LLM Agent จะสามารถเข้าใจคำสั่งภาษาธรรมชาติได้ดี แต่ยังคงมีข้อจำกัดสำคัญเมื่อทำงานร่วมกับเครื่องมือ CRM ที่มีความซับซ้อน ได้แก่

- LLM Agent **เลือกใช้เครื่องมือไม่เหมาะสม**กับภารกิจ (Incorrect Tool Selection)
- ส่งพารามิเตอร์ไม่ครบ**หรือไม่ตรงกับ Schema** ของระบบ (Parameter Mismatch)
- เกิดความผิดพลาดซ้ำในกรณีที่ Tools ส่งผลลัพธ์กลับมาไม่สมบูรณ์
- ขาดกลไกควบคุมลำดับการทำงานและการตรวจสอบย้อนหลัง (Lack of Control & Auditability)

Expected Benefits

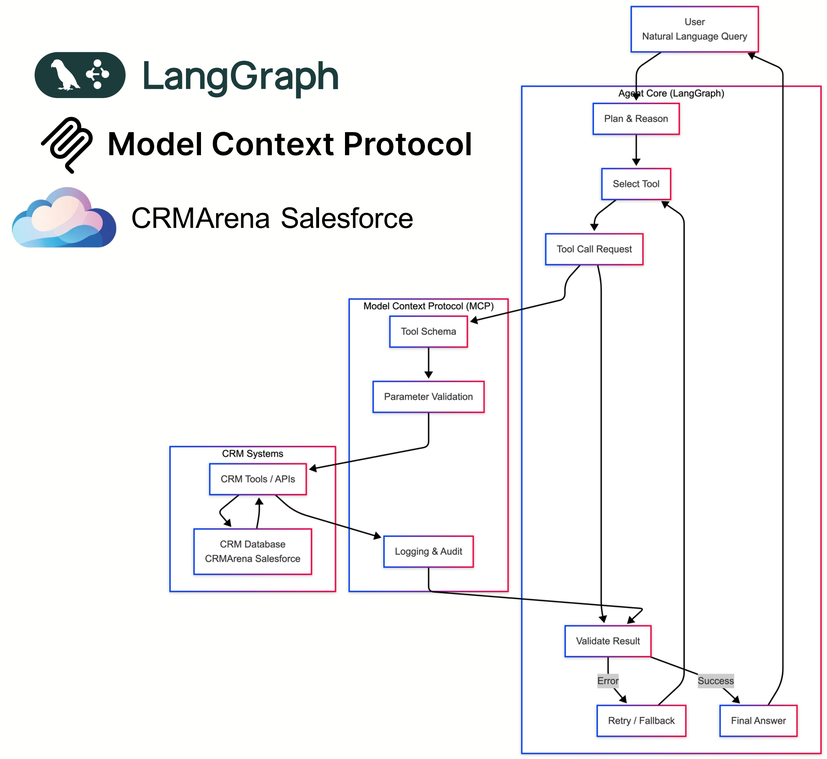
- ลดความผิดพลาดจาก Schema Mismatch และการเรียกใช้เครื่องมือผิด
- เพิ่มความสามารถในการตรวจสอบและติดตามการทำงานของ Agent
- รองรับการจัดการข้อผิดพลาดและ Retry อย่างเป็นระบบ
- เหมาะสำหรับการนำไปใช้ในระบบ CRM ที่มีความซับซ้อนสูง

About Project & CV

Methodology

ระบบถูกออกแบบให้ LLM Agent ทำงานภายใต้โครงสร้างเป็นลำดับขั้น โดยใช้สถาปัตยกรรม **Graph-Based Control (LangGraph)** เพื่อกำหนดกระบวนการตั้งแต่การวิเคราะห์คำถาม การเลือกและดึง Schema ของเครื่องมือ CRM การสร้างและเรียกใช้งานคำสั่ง ไปจนถึงการตรวจสอบผลลัพธ์และการ Retry เมื่อเกิดข้อผิดพลาด

การเชื่อมต่อระหว่าง **LLM กับเครื่องมือ CRM** ดำเนินการผ่าน **Model Context Protocol (MCP)** เพื่อกำหนด Schema การตรวจสอบพารามิเตอร์ และขอบเขตการใช้งานอย่างเป็นมาตรฐานเดียวกัน ระบบถูกออกแบบให้รองรับการทำงานแบบหลายขั้นตอนและสามารถควบคุม ตรวจสอบ และจัดการข้อผิดพลาดของ Agent ได้อย่างเป็นระบบ



Overview System Architecture

Future Work

- ประเมินประสิทธิภาพของ Agent บน CRM benchmark (CRMArena)
- เปรียบเทียบการทำงานระหว่าง LLM & API และ LLM & MCP
- ขยายภารกิจจาก Knowledge QA ไปสู่ CRM Analytics และ Multi-Step Actions

Senior Project