UNIVERSITÀ DEGLI STUDI ROMA TRE

Dipartimento di Ingegneria Civile, Informatica
e delle Tecnologie Aeronautiche

Corso di Laurea in Ingegneria Informatica

Aumentare le capacità di un chatbot usando Model Context Protocol (MCP)

Anno Accademico 2024/2025

Laureando

Del Prete Andrea

Matricola 589453

Relatore

Prof. Paolo Merialdo

Tutor

Dott. Di Nardo Giorgio

Indice

Indice **1**

Introduzione **2**

1 Capitolo 1 **4**

1.1 Questa è una Sezione 4

1.1.1 Questa è una Sottosezione 4

Conclusioni **5**

Ringraziamenti **6**

Bibliografia **7**

Introduzione

Siamo oramai in un'era in cui l'intelligenza artificiale è presente in ogni aspetto della nostra vita digitale, ancora di più dopo l'uscita di ChatGPT, che infranse il record di applicazione con la più rapida crescita nella storia di Internet, ben 100 milioni di utenti in soli 2 mesi [1]. Gli ultimi anni sono stati infatti caratterizzati da questi modelli generativi, i cosiddetti Large Language Model (LLM), letteralmente modelli linguistici di grandi dimensioni, in grado di simulare con sorprendente accuratezza le capacità conversazionali di un essere umano.

Un'interessante conseguenza del modo in cui questi sistemi sono stati creati, ma soprattutto la mole di dati usata per addestrarli, è stato l'emergere di comportamenti che potremmo considerare intelligenti, analoghi a qualcosa che una persona farebbe, non di certo una macchina. Ad esempio, i LLM sono in grado di comprendere il contesto, ragionare su problemi complessi e generare risposte articolate, mostrando una flessibilità che va ben oltre la semplice automazione.

Per rendere ancora più sofisticate le abilità di questi modelli linguistici, finora relegate a semplici chatbot che rispondono ai messaggi degli utenti, Anthropic, azienda leader nel settore della ricerca di LLM e creatrice dei molto diffusi modelli Claude Sonnet, ha ideato un meccanismo innovativo: il Model Context Protocol (MCP). Questo protocollo rappresenta un passo avanti fondamentale, poiché permette ai modelli linguistici di interfacciarsi con il mondo esterno in modo controllato e sicuro, eseguendo azioni predeterminate e accedendo a informazioni aggiornate o servizi specifici.

Il Model Context Protocol nasce dall'esigenza di superare i limiti dei LLM tradi-

zionali, che operano esclusivamente sulla base del testo fornito dall'utente e della conoscenza acquisita durante l'addestramento. Grazie a MCP, i modelli possono ricevere istruzioni strutturate, accedere a strumenti esterni, e persino collaborare con altri sistemi, ampliando notevolmente il loro campo di applicazione. Questo protocollo apre la strada a una nuova generazione di intelligenze artificiali, capaci non solo di dialogare, ma anche di agire e interagire in modo dinamico con l'ambiente digitale, rendendo possibile una vera integrazione tra AI e software tradizionali.
In questa tesi verrà analizzato il funzionamento del Model Context Protocol, le sue potenzialità e le implicazioni che comporta per il futuro dell'intelligenza artificiale, con particolare attenzione agli aspetti di sicurezza, etica e impatto sociale. Verranno inoltre esplorati casi d'uso pratici e scenari futuri, per comprendere appieno come questa innovazione possa trasformare il nostro rapporto con la tecnologia e quali sfide potrebbero sorgere nel suo percorso di diffusione e implementazione.

1

Capitolo 1

1.1 Questa è una Sezione

1.1.1 Questa è una Sottosezione

Conclusioni

Ringraziamenti

Grazie a tutti

Bibliografia

[1] UBS. Latest house view daily, 2023. URL: https://www.ubs.com/global/en/wealthmanagement/insights/chief-investment-office/house-view/daily/2023/latest-25052023.html.