Come funziona Clawdbot (Moltbot), l’AI opensource che fa cose

Nelle ultime settimane nel mondo tecnologico non fa altro che parlare di **Clawdbot** (da pochissimo ribattezzato **Moltbot** perché suonava troppo simile a Claude).

Cos’è Clawdbot (Moltbot

Clawdbot è un assistente personale AI open-source, auto-ospitato, creato dallo sviluppatore **Peter Steinberger**. Diversamente dai chatbot basati su browser, Moltbot gira direttamente sull’hardware dell’utente—da computer desktop a dispositivi compatti come Raspberry Pi—e si collega a piattaforme di messaggistica popolari come Whatsapp, Telegram, Discord, Slack e iMessage.

Come funziona l’agente Clawdbot (Moltbot)

Il funzionamento di Clawdbot si basa su un’architettura modulare. L’agente utilizza uno o più modelli di AI come motore di ragionamento e li combina con componenti che gli permettono di interagire con applicazioni reali. Può ricevere e inviare messaggi, accedere a file, gestire promemoria, leggere email o eseguire comandi, a seconda dei permessi concessi. Un elemento centrale è la memoria persistente, che consente all’agente di mantenere contesto e informazioni nel tempo.

Uno degli aspetti distintivi di Clawdbot è la capacità di integrarsi con piattaforme di messaggistica e strumenti di lavoro quotidiani. L'agente può essere configurato per operare tramite canali già utilizzati dagli utenti, diventando una sorta di interfaccia unica verso più servizi. Questo approccio rende l'automazione più fluida, ma allo stesso tempo aumenta la superficie di esposizione del sistema.

Il tema della sicurezza e della responsabilità

La natura auto-ospitata di Clawdbot sposta la responsabilità della sicurezza interamente sull'utente o sull'organizzazione che lo utilizza. Installazioni non protette o configurate in modo improprio possono risultare accessibili dall'esterno. In questi casi, l'agente può esporre conversazioni, dati operativi, credenziali e chiavi API, con conseguenze rilevanti in termini di violazioni e accessi non autorizzati.

L'uso di un agente AI operativo introduce anche un tema di governance. Quando un sistema prende decisioni ed esegue azioni sulla base di istruzioni in linguaggio naturale, diventa più complesso stabilire responsabilità, tracciabilità e controllo. In ambito aziendale questo solleva interrogativi su audit, compliance e gestione del rischio, soprattutto se l'agente opera su dati sensibili o processi critici.

Un segnale dell'evoluzione dell'AI

Clawdbot rappresenta un esempio concreto dell'evoluzione in corso nell'ecosistema AI: da strumenti conversazionali a soggetti capaci di agire. L'auto-hosting offre maggiore controllo e flessibilità, ma richiede competenze tecniche e un approccio maturo alla sicurezza. Senza adeguate misure di isolamento, autenticazione e monitoraggio, il rischio è che l'agente diventi un punto di vulnerabilità anziché un fattore

di efficienza.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/come-funziona-clawdbot-moltbot-lai-open source-che-fa-cose/563547/