INNOVATION PARTNERSHIPS
UNIVERSITY OF MICHIGAN

MAISON technology

Technology number: 2025-022

Technology ID
2025-022

Category
Software
Engineering & Physical Sciences

Inventor
Waseem Al-khatib
Zaid Ghazal

Further information
Ashwathi Iyer
ashwathi@umich.edu

Learn more

OVERVIEW

MAISON secures sensitive data in AI interactions using lightweight NLP checks

- Ensures data privacy on user devices without network transmission, enhancing security
- Useful for corporate data security, employee compliance, safe AI usage, and privacy protection

BACKGROUND

Generative AI tools like ChatGPT revolutionize how users interact with technology, aiding in tasks from customer support to content creation. However, this increased use brings heightened risks of sensitive data exposure, as prompts and materials uploaded to these AI platforms may inadvertently contain confidential information. Historically, safeguarding such data required complex, server-based validation processes that introduced delays and potential vulnerabilities during data transmission. These approaches often proved cumbersome and inefficient, particularly for on-the-go users needing quick AI assistance. An improved method is essential to ensure real-time data privacy without compromising user convenience, especially for organizations juggling large volumes of sensitive material.

INNOVATION

Researchers have created a software solution named MAISON that leverages lightweight Natural Language Processing (NLP) to validate and check data for sensitivity before it is

uploaded to generative AI tools. Running all validations directly on the user's device, MAISON ensures that no sensitive information leaves the user's RAM and CPU, thus, preventing data leaks. This technological advance allows MAISON to operate as a browser extension, keeping all computations internal and secure. The system can block, warn, or allow submissions, and even mask predefined sensitive details from being exposed. This innovation empowers companies, teams, and individuals to safely utilize AI technologies while retaining on-premises control over data exposure, making it useful for corporate data security, employee compliance, safe AI interactions, and maintaining privacy in a digital age.