Access Controlled Website Interaction for Agentic AI with Delegated Critical Tasks

Sunyoung Kim, Computer Science
Mentor: Hokeun Kim, Assistant Professor
School of Computing and Augmented intelligence

Motivation

- The recent advances of AI agents, autonomous systems capable of perceiving, reasoning, and executing tasks, raises new security concerns [1]. Their ability to access and control external resources demands robust and real-time access management to prevent misuse or unintended behavior.
- However, current e-commerce websites lack a standardized access control system to delegate authority to agentic AI.

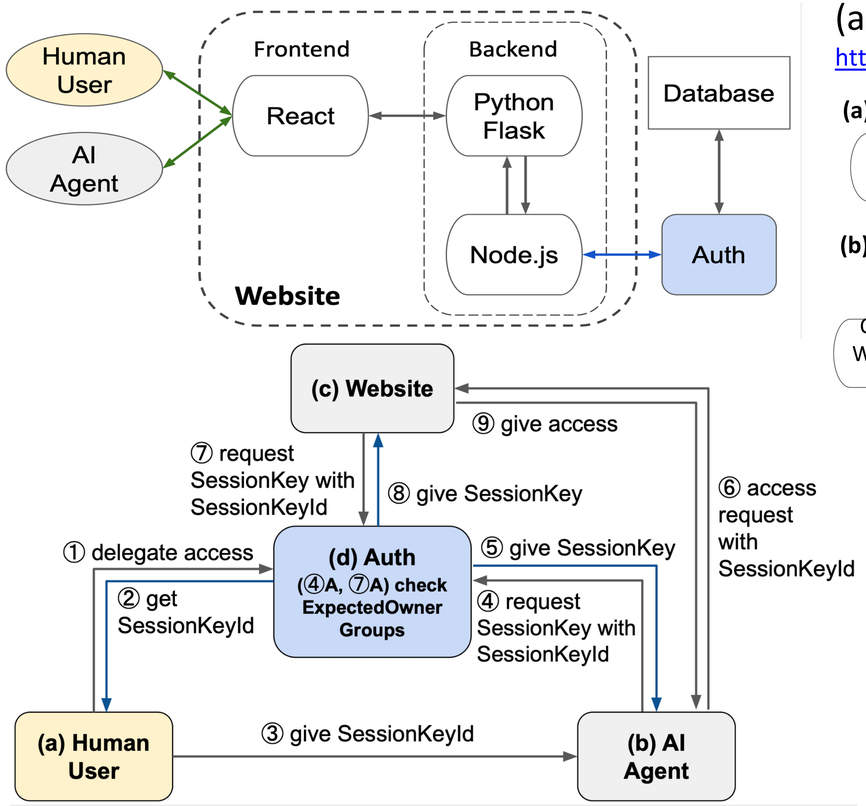
Background

Prior work proposed **Secure Swarm Tool (SST)** [2], an open-source decentralized security framework that uses local authorization entities (Auths) to manage trust and ensure secure communication among distributed devices.

References

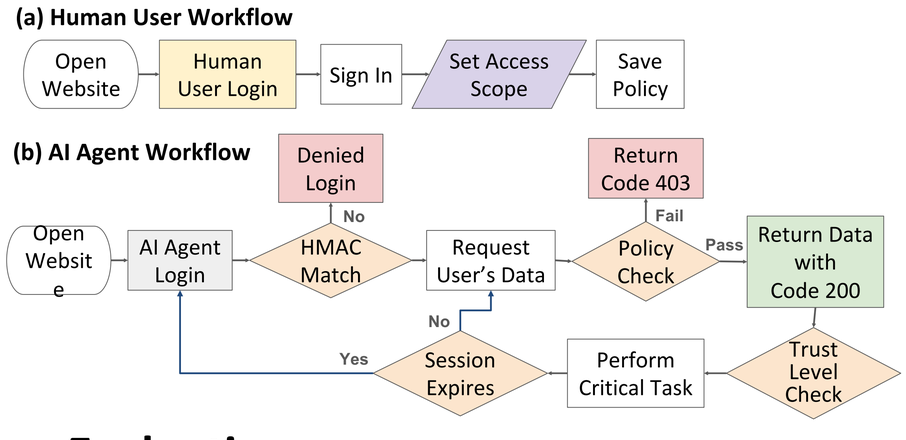
[1] Z. Deng et al. 2025. AI Agents Under Threat: A Survey of Key Security Challenges and Future Pathways. ACM Comput. Surv. 57, 7, Article 182 (Jul 2025), 36 pages. https://doi.org/10.1145/3716628
[2] H. Kim et al. 2020. Resilient Authentication and Authorization for the Internet of Things (IoT) Using Edge Computing. ACM TIOT 1, 1, Article 4 (Feb 2020), 27 pages. https://doi.org/10.1145/3375837
[3] S. Kim and H. Kim, "Access Controlled Website Interaction for Agentic AI with Delegated Critical Tasks," ACM WWW 2026. Dubai, UAE, Jun-Jul, 2026.

Proposed Approach and Design



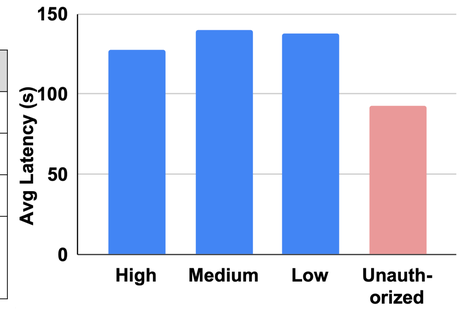
We design the website structure to provide secure and fine-grained access delegation by bringing in SST in the workflow. By combining user-defined policy enforcement, HMAC verification with the session key, and trust-based session management, the website ensures that autonomous agents operate strictly within their delegated authority. [3]

Proposed website workflows from the perspective of (a) human users and (b) AI agents.
https://github.com/asu-kim/agentic-website/blob/main/website/README.md



Evaluation

Agent	Average	Std
High	127,248.80	11,330
Medium	140,060.20	17,407
Low	137,842.40	6,733
Unauth-orized	92,793.60	11,781



We evaluate end-to-end latency, showing that rejected unauthorized requests are blocked efficiently within a short period of time. [3]
The medium- and low-trust agents show slightly higher latency due to variability in the agent-side LLM inference time, not due to the trust levels.