THE ACM WEB CONFERENCE 2026
29 June - 3 July 2026
Dubai, United Arab Emirates
www2026.thewebconf.org
Virtual EVENT

Access Controlled Website Interaction for Agentic AI with Delegated Critical Tasks

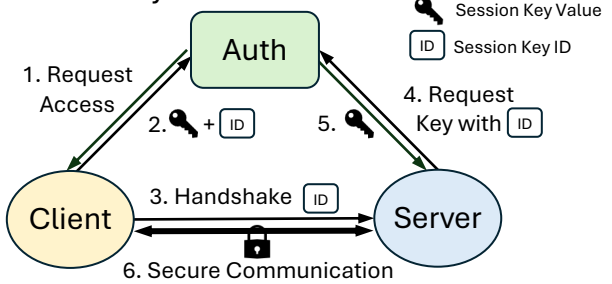
Sunyoung Kim and Hokeun Kim
Arizona State University

MOTIVATION

- The recent advances of AI agents, autonomous systems capable of perceiving, reasoning, and executing tasks, raise 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 [2].

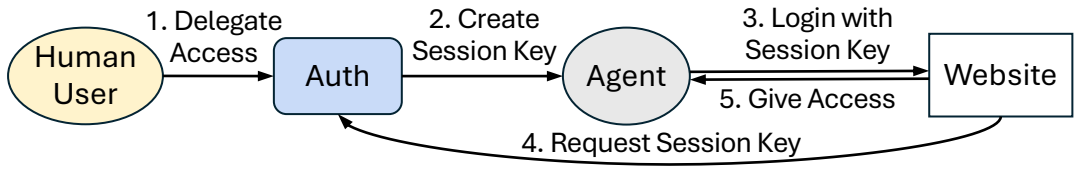
BACKGROUND

Secure Swarm Toolkit (SST) [3] is an open-source decentralized security framework. **Auth** acts as a Key Distribution Center (KDC) and issues cryptographic session keys.

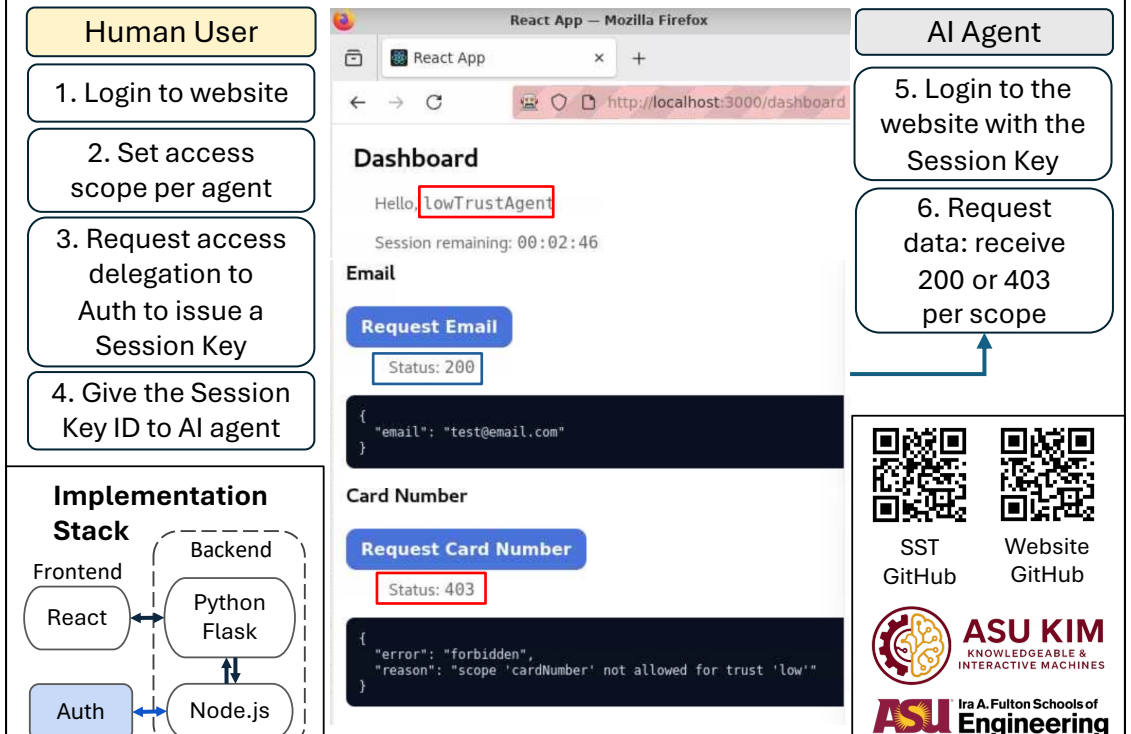


PROPOSED APPROACH & DESIGN

Overall Workflow



Website Design and Interaction



Implementation Stack

SST GitHub

Website GitHub

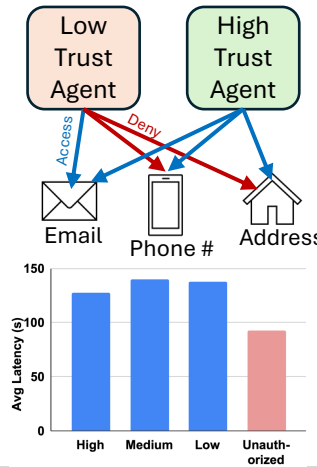
ASU KIM KNOWLEDGEABLE & INTERACTIVE MACHINES

Ira A. Fulton Schools of Engineering Arizona State University

EVALUATION

- **Correctness** and **latency** evaluation
- Tested on ASU Sol Supercomputer (NVIDIA A100 GPU)
- GPT-OSS-20B for Agent Reasoning
- Firefox Browser

Evaluation Aspect	Result
Authentication	✓ 100% Success
Access Control	✓ Access Scopes Enforced
Unauthorized Requests	✓ 100% Rejected
Repeated Key Requests	✓ 100% Rejected
Session Expiration	✓ Auto Logout



REFERENCES & ACKNOWLEDGMENT

[1] Deng, Zehang, et al. "AI agents under threat: A survey of key security challenges and future pathways." *ACM Computing Surveys* 57.7 (2025): 1-36.
[2] Kim, Sunyoung, and Kim, Hokeun. "A Case Study on Delegating Critical Tasks to Agentic AI and Prototype Access Control Methods." *2025 CARS*. IEEE, 2025.
[3] Kim, Hokeun, et al. "A toolkit for construction of authorization service infrastructure for the internet of things." *Proceedings of the second international conference on IoTDI*. 2017.
Acknowledgment: This work was supported in part by the NSF grant POSE-#2449200.