

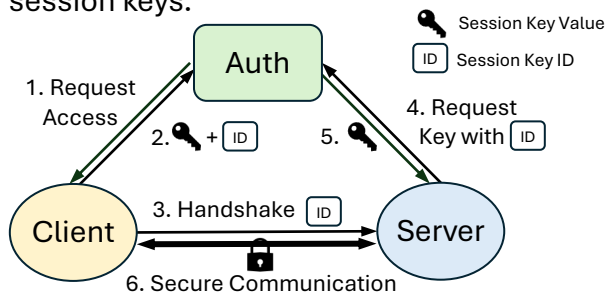


MOTIVATION

- 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].

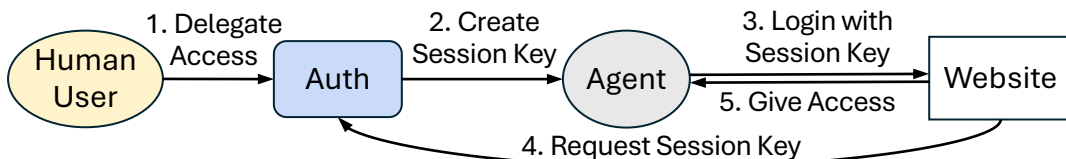
BACKGROUND

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

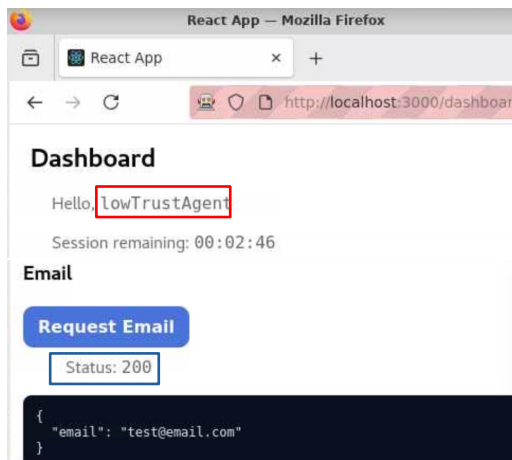
Overall Workflow



Website Design and Interaction

Human User

1. Login to website
2. Set access scope per agent
3. Request access delegation to Auth to issue a Session Key
4. Give the Session Key ID to AI agent



Dashboard

Hello, LowTrustAgent

Session remaining: 00:02:46

Email

Request Email

Status: 200

```
{
  "email": "test@email.com"
}
```

Card Number

Request Card Number

Status: 403

```
{
  "error": "forbidden",
  "reason": "'scope 'cardNumber' not allowed for trust 'low'"
}
```

AI Agent

5. Login to the website with the Session Key
6. Request data: receive 200 or 403 per scope

Implementation Stack

Frontend

React

Backend

Python Flask

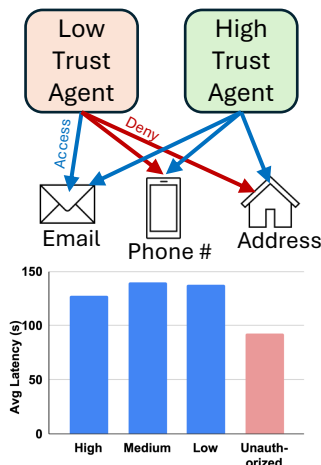
Node.js

Auth

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.