Arizona State University

CCS-LAMPS 2026

ASU KIM
KNOWLEDGEABLE & INTERACTIVE MACHINES

Design Exploration for Context-Based Access Control of Vision-Language-Action Model-Based Embodied Agents

Krutyanjay Shinde, Dongha Kim, and Hokeun Kim

School of Computing and Augmented Intelligence,
Arizona State University

LAMPS '26 · November 15, 2026 · The Hague, Netherlands

Motivation

- VLA models connect perception and language to physical actuation.
- Manipulated inputs or a compromised VLA model can produce policy-violating robot actions.
- These actions can have **hazardous physical consequences**, including unsafe motion near people.

Access control is needed before physical execution.

Why Context-Based Authorization?

VLA access control must account for current runtime context.

Example policy: permit operation only…

- in a designated location,
- during an allowed time period,
- when no people are nearby.

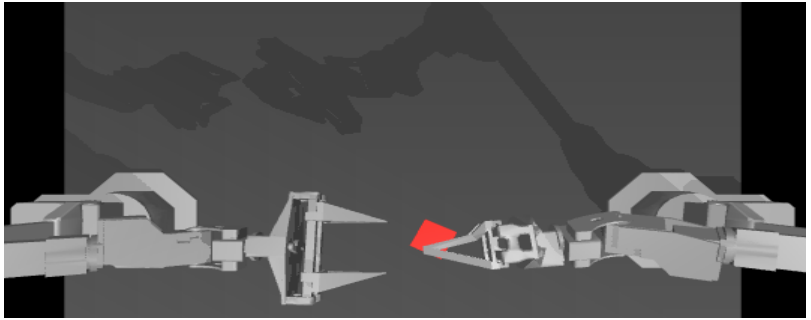
The same action may be permitted in one context and denied in another.

Challenge: check runtime context while meeting latency constraints.

Background: openpi & SST

openpi & π_0-FAST

- π_0-FAST: autoregressive VLA model for robotic control.
- openpi hosts its policy server.
- WebSockets connect it to the MuJoCo ALOHA simulator.



Secure Swarm Toolkit (SST)

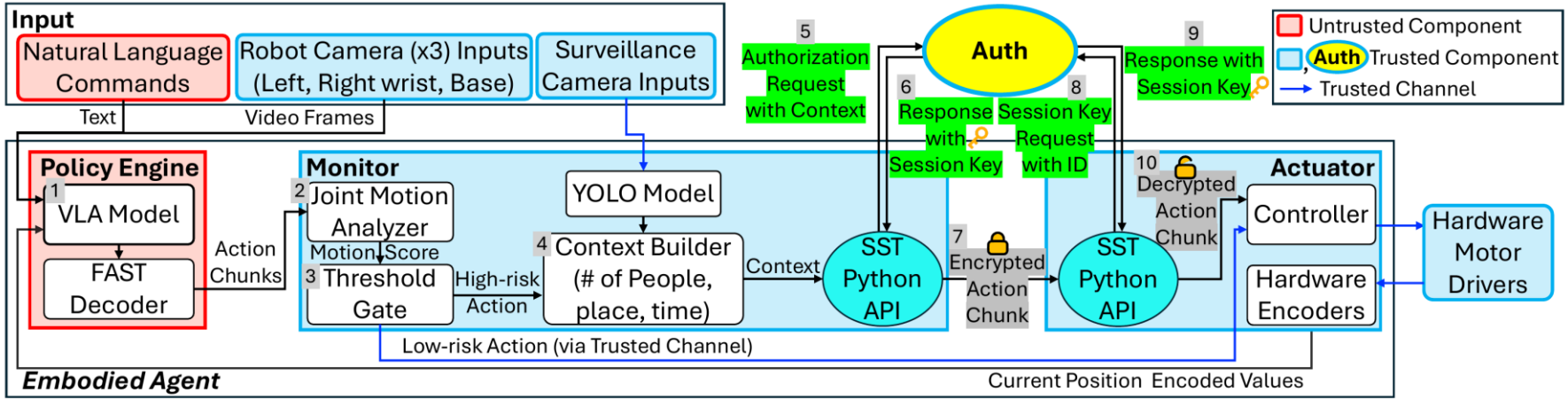
- Open-source framework for distributed authentication and authorization.
- Auth manages and distributes cryptographic keys for registered devices.



github.com/
iotauth/iotauth

Framework Overview

The Monitor connects VLA action generation to context-based authorization and execution.



VLA generates actions. Monitor, Auth, and Actuator control execution.

Joint Motion Analysis

Action chunk: a sequence of predicted future robot commands

- **Intra-chunk**: max–min command captures motion within the chunk, including out-and-back movement.
- **Inter-chunk**: current pose to the first new command captures a jump into the chunk.
- Normalize by each joint's range. Take the maximum across both measures and all joints.

$$d_j^{\text{intra}} = \frac{\max_k a_{t,k,j} - \min_k a_{t,k,j}}{R_j}$$

$$d_j^{\text{inter}} = \frac{|a_{t,0,j} - q_{t,j}|}{R_j}$$

$$S_{\text{motion}} = \max_j \left[\max\left(d_j^{\text{intra}}, d_j^{\text{inter}} \right) \right]$$

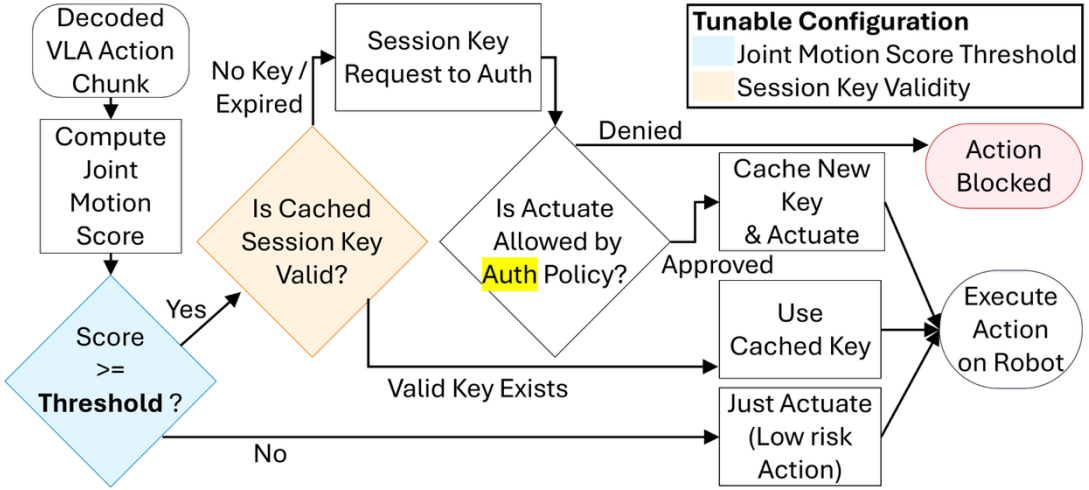
R_j: joint's physical range

S < τ: Low-risk

S ≥ τ: High-risk

Motion score triggers authorization; it does not guarantee physical safety.

Authorization Decision & Enforcement



- Low-risk: forward directly.
- High-risk: reuse a valid key or request authorization.
- Auth evaluates runtime context against policy.
- Permit: issue a key. Deny: block the action.

Monitor encrypts. Actuator retrieves the matching key and decrypts.

Design Choices

Motion threshold τ

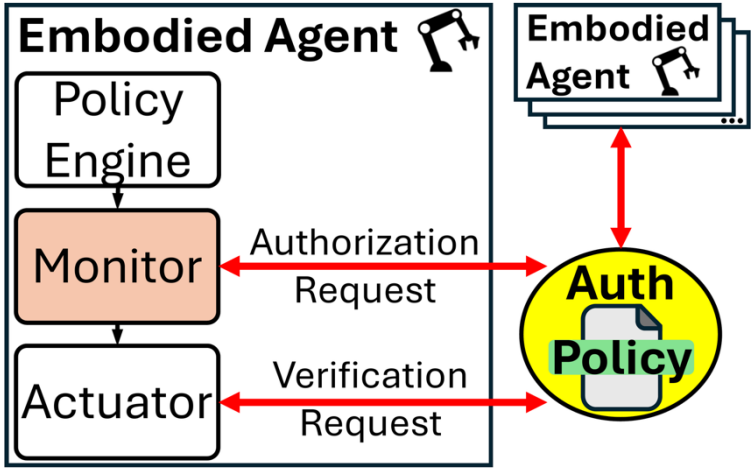
- **Higher τ**: more actions bypass authorization.
- **Lower τ**: more actions require authorization.

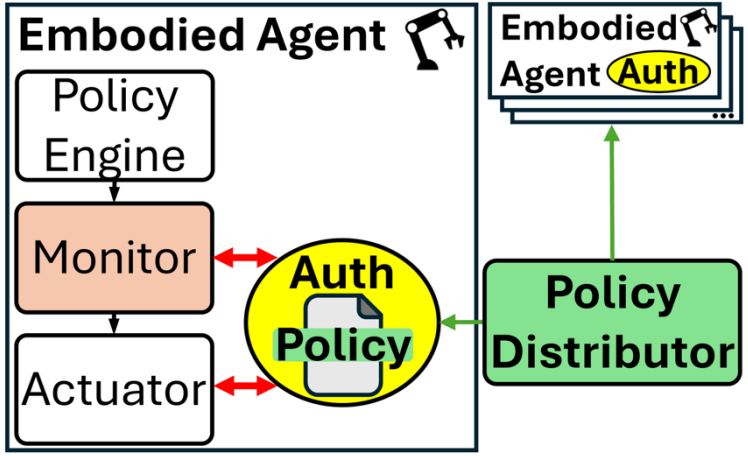
Session key validity t

- **Longer t**: more reuse of earlier authorization.
- **Shorter t**: more frequent context-based reauthorization.

Design Choices

Policy Decision Point outside vs. within of Embodied Agent





Outside (Centralized)

Remote Auth manages policy decisions.

Inside (Decentralized)

Local Auth, external policy distributor.

Experimental Setup

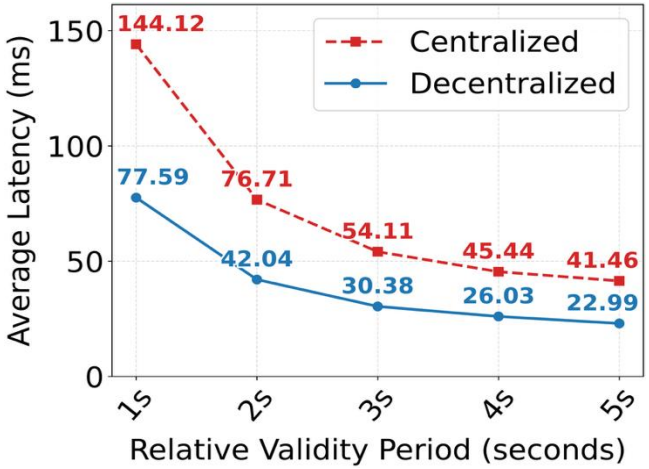
- π_0-FAST with the MuJoCo ALOHA simulator.
- Centralized: remote Auth over a wired LAN.
- 10 ms added one-way network delay.
- Decentralized: all components on the workstation to emulate on-board deployment.
- Parameter sweeps: 5 runs × 30 cycles per setting.

Measured interval

Monitor receives chunk → decrypted input reaches Actuator
VLA inference time excluded

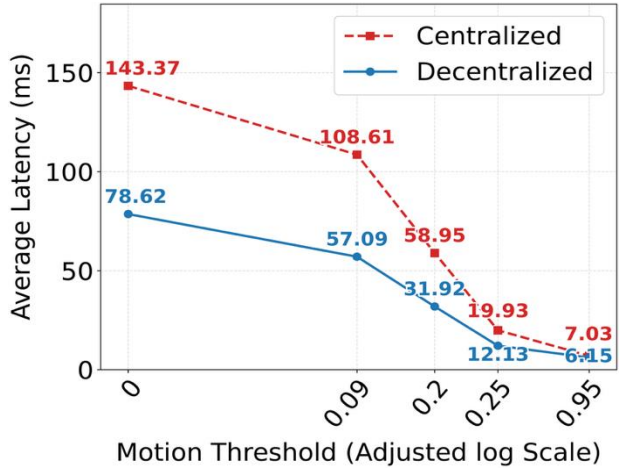
Results: Key Validity & Motion Threshold

Key validity sweep · τ = 0



Key reuse lowers mean latency.
144.12 → 41.46 ms centrally.

Threshold sweep · t = 1 s

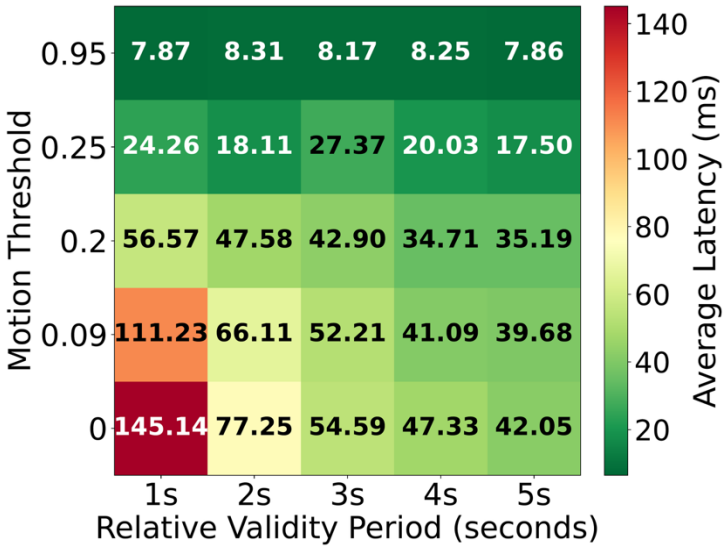


Higher τ reduces requests.
More chunks bypass Auth.

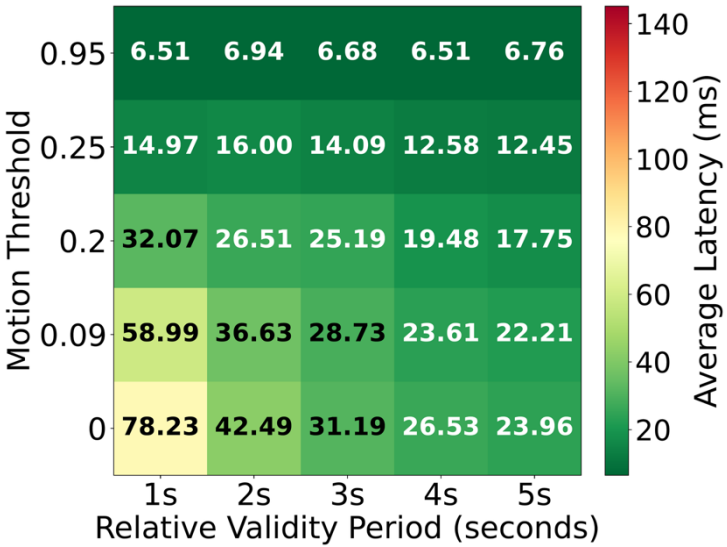
Observed maximum latency falls less than the mean when fresh authorization still occurs.

Results: Auth Placement

Centralized Auth



Decentralized Auth



τ = 0, t = 1 s: 145.14 ms centralized / 78.23 ms decentralized

Local Auth avoids remote network round trips.

Conclusion

- Context-based authorization connects VLA action generation to controlled execution.
- Motion threshold and key validity reduce latency through different mechanisms.
- Decentralized Auth avoids remote network round trips.

Thank you · Questions?

Authors:
Krutyanjay Shinde, **Dongha Kim**, and Hokeun Kim
Contact:
kshinde6@asu.edu, dongha@asu.edu, hokeun@asu.edu

Websites:
- https://labs.engineering.asu.edu/kim/
- https://jakio815.github.io/
- https://hokeun.github.io/