ZETAS: Zero Trust Framework for Autonomous Systems with Shared Cyber Attack Surfaces

Soham Vaidya
NTU & I²R, A*STAR

Anku Adhikari
I²R, A*STAR

Background & Aim

Interconnected autonomous systems are rapidly emerging in domains like smart factories and healthcare. These systems, which have similar layered architectures (sensing, communication, control, and interface), include robots, drones, IoT sensors, AVs, and XR technology. As a result, there is a potential of lateral movement across the components and overlapping vulnerabilities.

To address this, Zero Trust Architecture (ZTA) can be used to enhance security. However, traditional ZTA in such environments can face limitations like:

- High computational and power demands.
- Latency from continuous authentication and policy checks.
- Centralized Policy Decision Points (PDPs), creating bottlenecks and a single point of failure.

Aim: We propose *ZETAS (Zero Trust for Autonomous Systems)* - a unified, Zero Trust framework tailored for autonomous systems to:

1. Enable low-latency real-time monitoring using lightweight AI models.
2. Support optimized mutual attestation.
3. Implement distributed PDPs to reduce latency and enhance resilience.

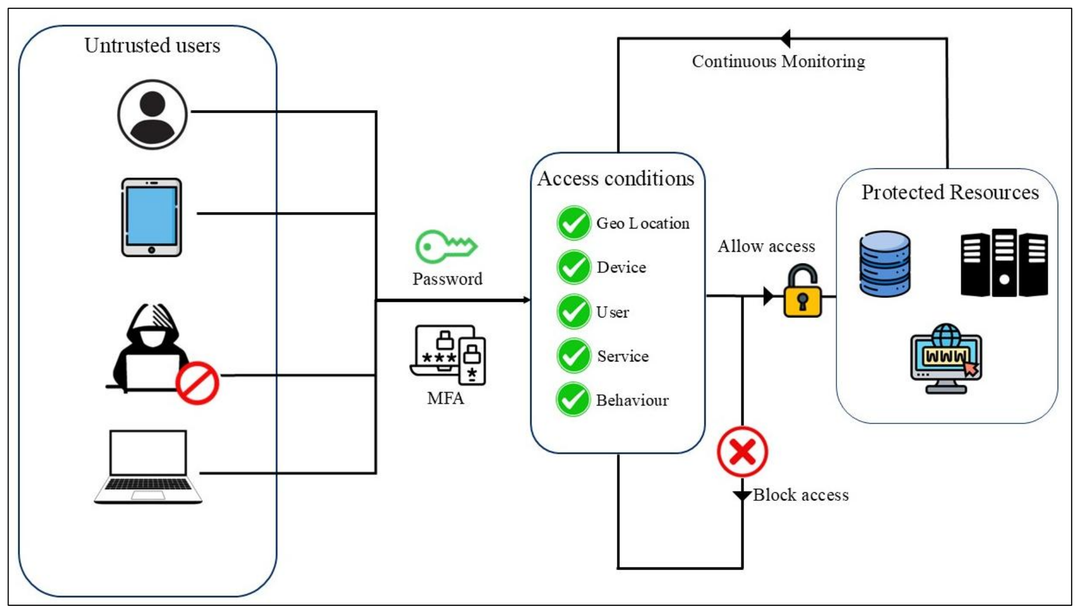
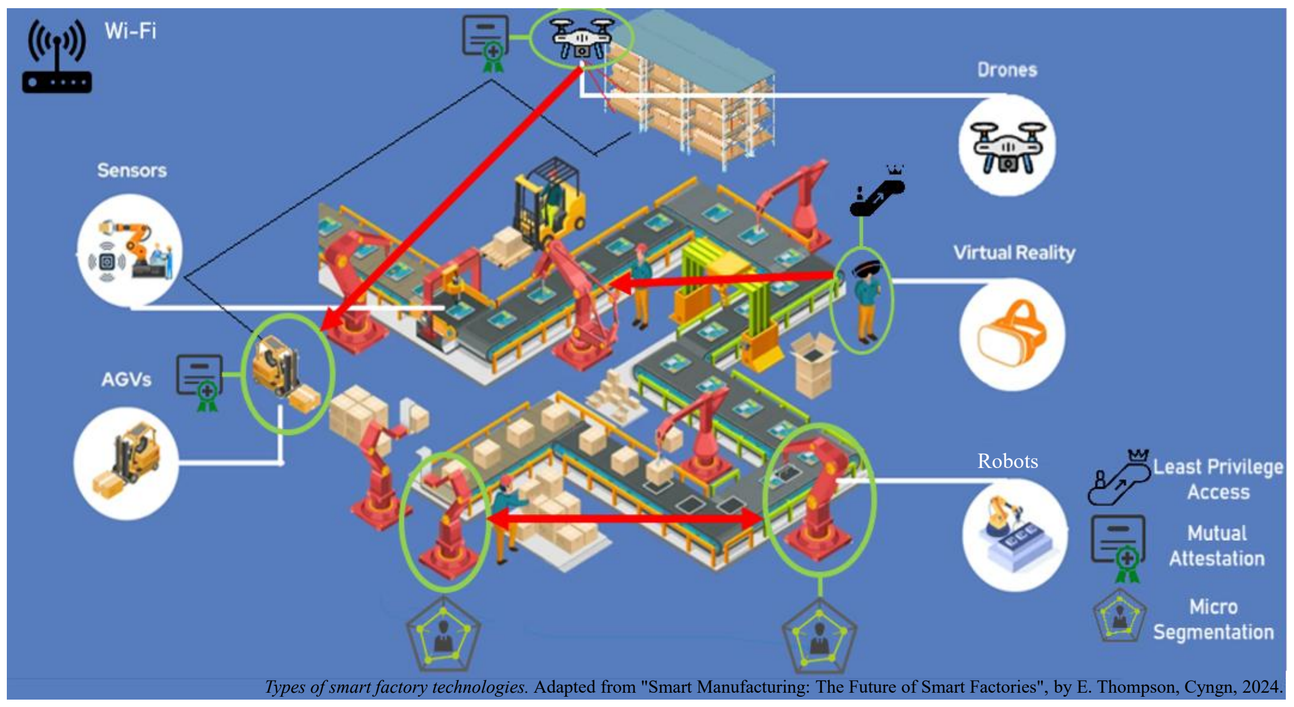


Figure 1: Zero Trust Architecture Diagram

Threat Model



Types of smart factory technologies. Adapted from "Smart Manufacturing: The Future of Smart Factories", by E. Thompson, Cyngn, 2024.

Figure 2: Proposed ZETAS framework for Smart Factory application

Survey and Analysis

Potential Attack	STRIDE	Impact	ZTA Defence
Command Injection from Compromised Wi-Fi → AGV	Tampering, Elevation of Privilege, Information Disclosure	Rogue navigation commands can cause collisions or data theft	*Continuous Monitoring + Mutual Attestation*
Spoofed Data Injection from Sensor → Robot	Spoofing, Tampering	Robots act on fake commands or manipulated sensor data	*Policy Enforcement Point (PEP) + Least Privilege Access*
Replay Attack from Compromised Camera → AGV	Tampering, Spoofing	Repeated actions cause inventory misplacement or redundant AGV movements	*Mutual Attestation + Continuous Monitoring*
Command Injection from XR Interface → Robots	Elevation of Privilege, Tampering, Repudiation	Malicious XR sends unauthorized start/stop or reprogramming commands	*Micro-segmentation + Least Privilege Access + Mutual Attestation*
Path Override from AGV → Robots	Tampering, Denial of Service	Factory Robot Arm follows incorrect path, risking collision or production halt	*Continuous Monitoring + Policy Enforcement Point (PEP)*

Methodology

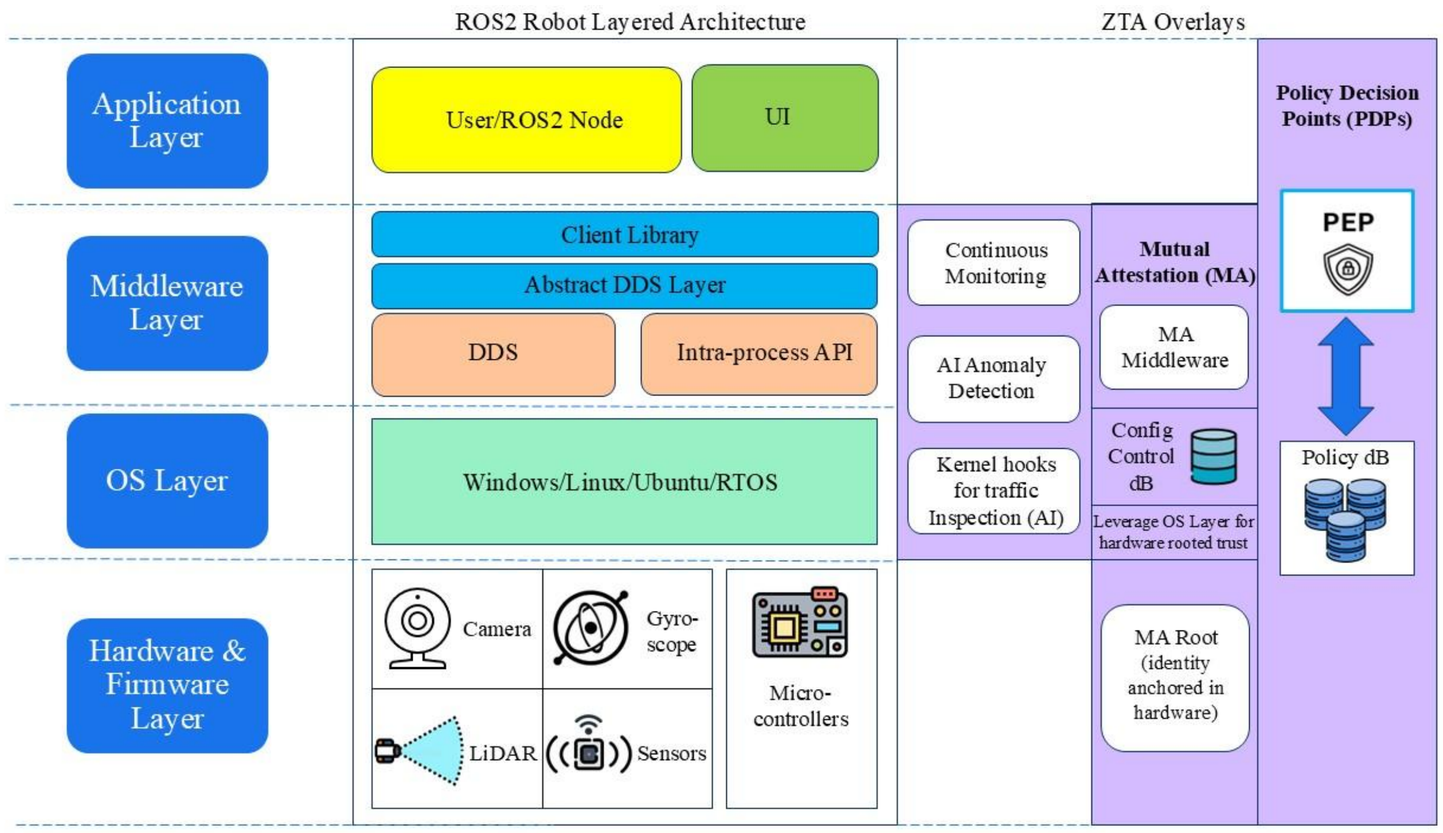


Figure 3: *ZETAS* framework overlays with ROS2 Architecture for robots

Challenges

1. Optimizing mutual attestation by using robust trust models that reduce the number of handshakes for authentication.
2. Managing distributed access and storage of the policy databases for Policy Decision Points (PDP).
3. Designing AI pipelines that balance inference accuracy with real-time performance constraints.
4. Quantizing models to fit memory and compute limits of embedded edge platform.
5. Establishing benchmarking metrics to evaluate trust model accuracy, latency, anomaly detection rates across diverse autonomous systems and operational scenarios.

Acknowledgement

This work was partly supported by the Singapore NRF Fellowship programme (NRF-NRFF16-2024-0002).

Connect!

More Info!