Poster: Identity-Independent IoT for Overarching Policy Enforcement

Luoyao Hao and Henning Schulzrinne
Department of Computer Science, Columbia University, New York, NY, USA
Email: {lyhao, hgs}@cs.columbia.edu

2024 IEEE Security and Privacy Workshops (SPW) | 979-8-3503-5487-4/24/$31.00 ©2024 IEEE | DOI: 10.1109/SPW63631.2024.00036

***Abstract*—Enforcing overarching policies such as safety norms and energy restrictions becomes critical as IoT scales and integrates into large systems. These policies should be applied preemptively and capable of adapting to system changes. Traditional IoT systems, reliant on fixed device identities, limit reliability, scalability, and resilience. Thus, we propose Identity-Independent IoT (I3oT), centered on adopting flexible descriptors to enforce policies. I3oT introduces a separate management plane on top of the standard operational workflow, thereby enhancing safety in scalable and integrated IoT systems.**

I. Introduction

IoT aims to enable seamless interconnectivity of everyday objects, turning them into a cohesive system. This goes beyond "Do It Yourself" (DIY) individual devices but lies in system-wide automation and integration. Yet, the growing mix of heterogeneous devices and their complex automation necessitates a clear need for structured governance to ensure that operations, data, and system changes comply with established safety protocols, preventing system disruptions caused by irregular behaviors or data errors [1].

However, today's large-scale IoT systems lack a systematic approach to enforce overarching policies (e.g., safety norms, energy limits, expected behaviors) that are often set by regulatory agencies, manufacturers, and development communities. Consider a smart building where fire door operations could be governed by policies from the fire department and building regulators. Such policies must be enforced without prior knowledge of specific device identities.

Thus, we propose Identity-Independent IoT (I3oT) and a distinct separation of IoT management and operation. I3oT focuses on using relationships and properties, instead of identities, for policy enforcement. The management plane oversees the operation plane, with capabilities to approve, deny, override, or double-check operations. It ensures all actions and system changes align with established policies, enhancing safety and regulatory compliance in IoT systems.

II. I3oT: Design and Architecture

I3oT identifies devices based on properties and inter-entity relationships, and thus achieves identity-independence. This is essential for enforcing overarching policies that are preferably configured before introducing devices (e.g., fire code compliance for any device at all times).

This work is supported by the National Science Foundation under grants CNS-1932418 and EEC-2133516.

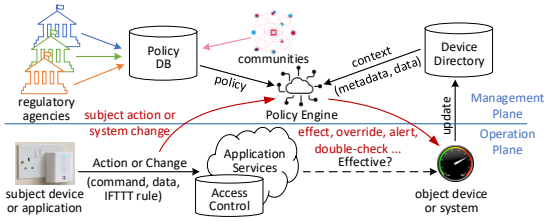

Fig. 1. Separation between IoT management and operation.

We design an I3oT-based policy specification and a policy server to process policies independent of device identities. A policy essentially defines the evaluation criteria for system changes (e.g., device actions, data inputs, event scheduling) and the necessary context for assessment. For example, "<action: turn on, subject: {type: AC}, object: {type: heater, status: on}, relationship: AC.feed==heater.feed, result: warning>" issues a warning when activating any AC in an area with a working heater, potentially violating energy-saving restrictions. Existing ontologies, such as Brick[1] and WoT[2], should be adopted to define properties and relationships.

Additionally, I3oT features a novel architecture with separate management and operation planes. As shown in Fig. 1, the operation plane handles standard IoT workflows, while the management plane, comprising a Policy Database, Policy Engine, and Device Directory [2], [3], enforces policies. This architecture ensures actions on the operation plane align with policies from authoritative bodies, covering fire codes, electrical guidelines, and device-specific regulations. The interplay between these elements results in a structured decision-making process, to approve, deny, override, or double-check operations, ensuring compliance and safety in IoT systems.

III. Conclusion

We outline I3oT and design a management plane to enforce overarching policies. I3oT offers significant advantages, including forward compatibility, compact and reusable policy set, and integration of regulatory bodies into IoT ecosystems.

References

[1] Z. B. Celik, G. Tan, and P. D. McDaniel, "IoTGuard: Dynamic enforcement of security and safety policy in commodity IoT," in *NDSS*, 2019.
[2] L. Hao and H. Schulzrinne, "Goldie: Harmonization and orchestration towards a global directory for IoT," in *IEEE INFOCOM*, 2021.
[3] L. Hao, V. Naik, and H. Schulzrinne, "DBAC: Directory-based access control for geographically distributed IoT systems," in *IEEE INFOCOM*, 2022, pp. 360–369.

[1]https://brickschema.org/
[2]https://www.w3.org/TR/wot-thing-description11/

DOI 10.1109/SPW63631.2024.00036