A Middleware for Secure Integration of Heterogeneous Edge Devices

Arthur Desuert, Stéphanie Chollet, Laurent Pion, David Hély
Univ. Grenoble Alpes, Grenoble INP, LCIS, CTSYS Team, F-26000 Valence, France
{firstname.lastname}@lcis.grenoble-inp.fr

Context

Statement

Security is crucial in IoT environment, but connected devices have:

- ❑ **heterogeneous constraints** → Power, Cost
- ❑ **dynamic behaviors**
- ❑ **heterogenous security** → Authentication, Confidentiality, Integrity

How to guarantee
secure communication and access
to the connected devices?

Requirements

For smart-home use cases [1]:

- ❑ **manage heterogeneity** of the devices, their protocols and their security.
- ❑ **manage dynamism**, to handle smooth arrival and departure of devices.
- ❑ **handle security for all devices**, from high end to low cost.
- ❑ **provide convenient interfaces**, to ease pervasive application development.

Background

Device security

How security is managed in current IoT protocols?

	Authentication level	Authentication mean	Confidentiality and Integrity
Wi-Fi	Simple, mutual	Shared secret	Configuration dependant
zigbee	None, simple, mutual	Shared secret	Yes
BLE	None, simple, mutual	User validation	Configuration dependant

→ **Security is present but heterogeneous**

→ **Strong reliance on secrets**

How secrets are stored on the devices? [2]

	Security	Cost	Adoption
Flash	None	Low	High
Secure Element	High	High	Domain-specific
PUF	Moderate	Moderate	Low

→ **Lack of affordable yet secure solution for low cost devices**

→ **Can PUF be a complementary solution?**

Middleware

How do current middleware handle IoT challenges?

		Heterogeneity	Dynamism	Security
Cloud Middleware	By cloud providers companies: Microsoft, Amazon, Orange	~	−	+
Fog/Edge Middleware	Active research field: In.IoT, LinkSmart, iCASA	~	+	−

→ **Difficult integration of constrained devices**

→ **Limited dynamism management**

→ **Secure communication interfaces**

→ **Integration of constrained and unconstrained devices**

→ **Good dynamism management**

→ **Rarely secure communication interfaces**

→ **Can a middleware solution provide dynamic and secure management of heterogeneous devices?**

Approach

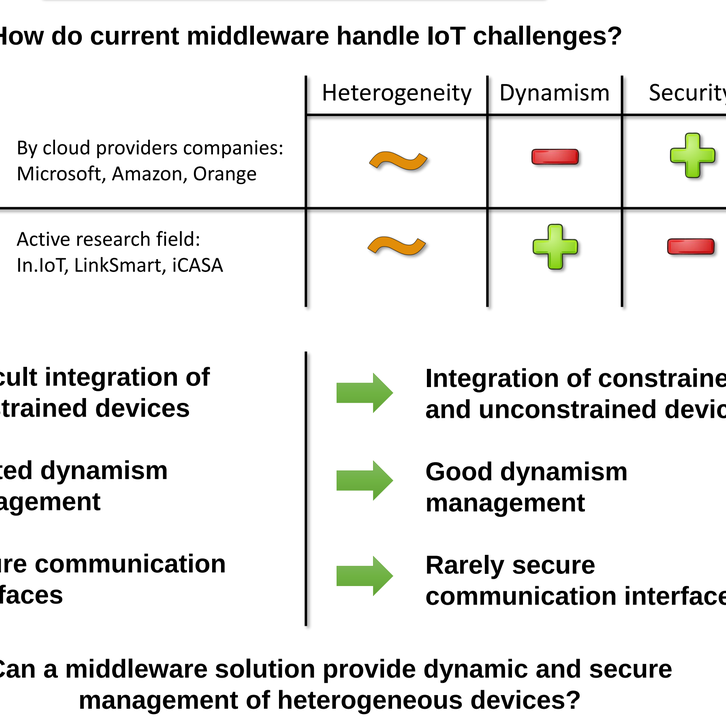
Fog middleware

Objective:

- ❑ facilitate the **secure communication and access** with connected devices while supporting their **heterogeneity** and **dynamism**.

Main characteristics:

- ❑ **secure by design** with secret management, authentication and secure protocols to provide end-to-end security from applications to devices.
- ❑ **security for every device**, with support of solutions adapted to various constraints and security requirements.
- ❑ **Service-Oriented Approach (SOA)** to abstract the complexity of the devices and their security, simplifying access for applications.
- ❑ **module-based architecture** to ease the dynamic integration of new protocols, improving heterogeneity and dynamism support.



→ **design of a PUF-based security protocol** [3] for devices.

→ **secure integration** of a wide range of heterogenous devices.

→ **low-coupling** between applications and devices.

Implementation and Validation

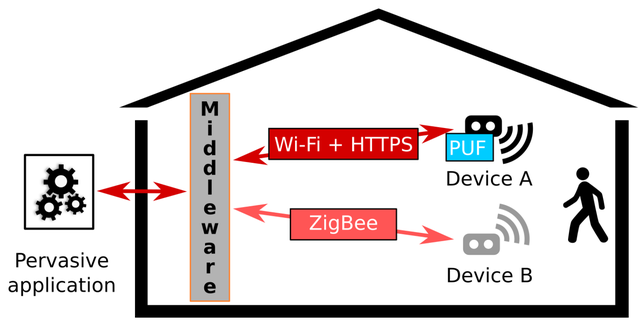
Implementation

Featured technologies:

- ❑ modules implemented as **micro-services** with a reactive Java framework.
- ❑ **secure REST interfaces** provided by modules using HTTPS with authentication mechanisms.
- ❑ publish/subscribe **secure communication** used between devices and the middleware.

Validation

Design and implementation of **validation scenarios**



References

[1] C. Escoffier, S. Chollet, and P. Lalanda, “Lessons learned in building pervasive platforms”, in *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)*, Jan. 2014, pp. 7–12.

[2] S. Chollet, L. Pion, N. Barbot, and C. Michel, “Secure IoT for a Pervasive Platform”, in *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Mar. 2018, pp. 113–118.

[3] **A. Desuert**, S. Chollet, L. Pion, and D. Hély, “Refillable PUF Authentication Protocol for Constrained Devices” in *Journal of Ambient Intelligence and Smart Environments*, accepted.

Acknowledgement: This project has received funding from the Trust Chair of the Grenoble-INP Foundation.