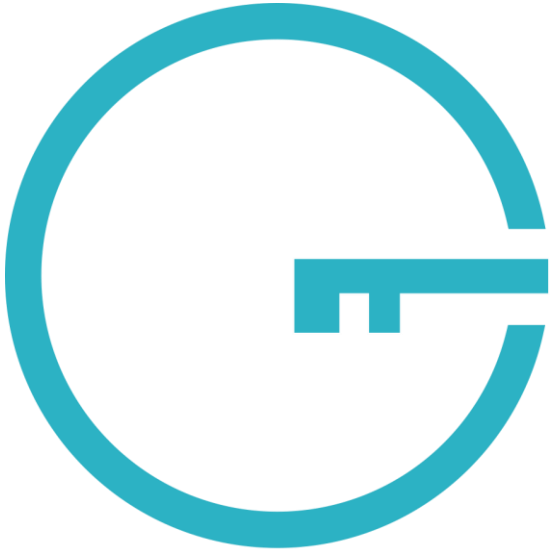
Safe-Guarding Home IoT Enviroments with Personalised Real-time Risk Control



GHOST

Dr. Marios Anagnostopoulos

Marios.Anagnostopoulos@ntnu.no

Norwegian University of Science and Technology (NTNU)

RELink – Oslo

11/06/2019

Partners:

Televes, NTNU, EXUS, KIT Karlsruher Institut für Technologie, kalos Information Systems, Université de Genève, iti, Imperial College London, OBRELA Security Industries, Cruz Roja Española

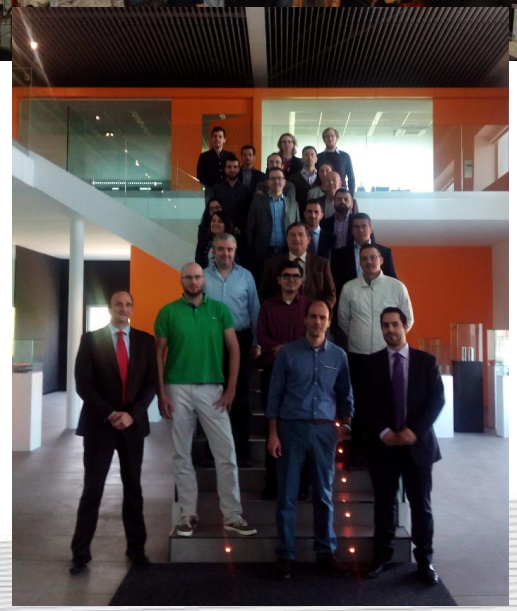
GHOST has received funding from the European Union's Horizon 2020 Framework Programme for Research and Innovation under GA No. 740923

Index

- Who are we?
- Main challenges for IoT security
- GHOST vision and mission
- GHOST high-level concept
- GHOST technical architecture
- GHOST key aspects

Who are we?

	ENTITY	TYPE
Televes	TELEVES (Spain)	Industrial partner (Midcap)
UNIVERSITÉ DE GENÈVE	University of Geneva (Switzerland)	Academic partner
iti	CERTH (Greece)	Academic partner
NTNU	NTNU (Norway)	Academic partner
Imperial College London	IMPERIAL COLLEGE (United Kingdom)	Academic partner
EXUS	EXUS (United Kingdom)	Industrial partner (SME)
KIT Karlsruher Institut für Technologie	Technical University of Darmstad (Germany)	Academic partner
kalos Information Systems	Kalos Information System (Norway and Romania)	Industrial partner (SME)
Cruz Roja Española	CRE (Spain)	NGO
OBRELA SECURITY INDUSTRIES	Obrela Security (Greece)	Industrial partner (SME)



Main challenges for IoT security

- **Cyber crime will cost 5.2$ trillion over the next five years**: https://www.information-age.com/cost-cybercrime-123478352/
- **61% of industries using IoT have already experienced an attack**: https://www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html
- **IoT attacks have increased 600% in the last year**: https://www.techrepublic.com/article/as-iot-attacks-increase-600-in-one-year-businesses-need-to-up-their-security/
- The **average** for **detecting** a data breach **is** currently **191 days**: https://www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html
- There are **not specific IoT-focused security solutions**
- IoT-enabled **home** solutions contain **critical information** for the user (health, energy, habits, etc.)

GHOST vision and mission

- Vision
  - GHOST envisions a **transparent cybersecurity** environment for all Europeans living in a connected world: with minimal effort consumers will become aware and **understand** the cybersecurity risks (threats and vulnerabilities), and will take informative decisions affecting their cyber-physical security and privacy. Cybersecurity technology will transform consumers' decisions into **reliable automated security services** and solutions, promote **security-friendly end-user habits** through behavioural engineering, and deliver **usable transparency**
- Mission
  - To deliver the first generation of **disruptive software-enabled usable security network solution for smart-home occupants**. GHOST cutting-edge technology will increase the level and the effectiveness of automation of existing cybersecurity services, enhance **system self-defence** and will open up the cybersecurity 'blackbox' to consumers and build **trust** through advanced usable transparency tools derived from end-users' mental models.

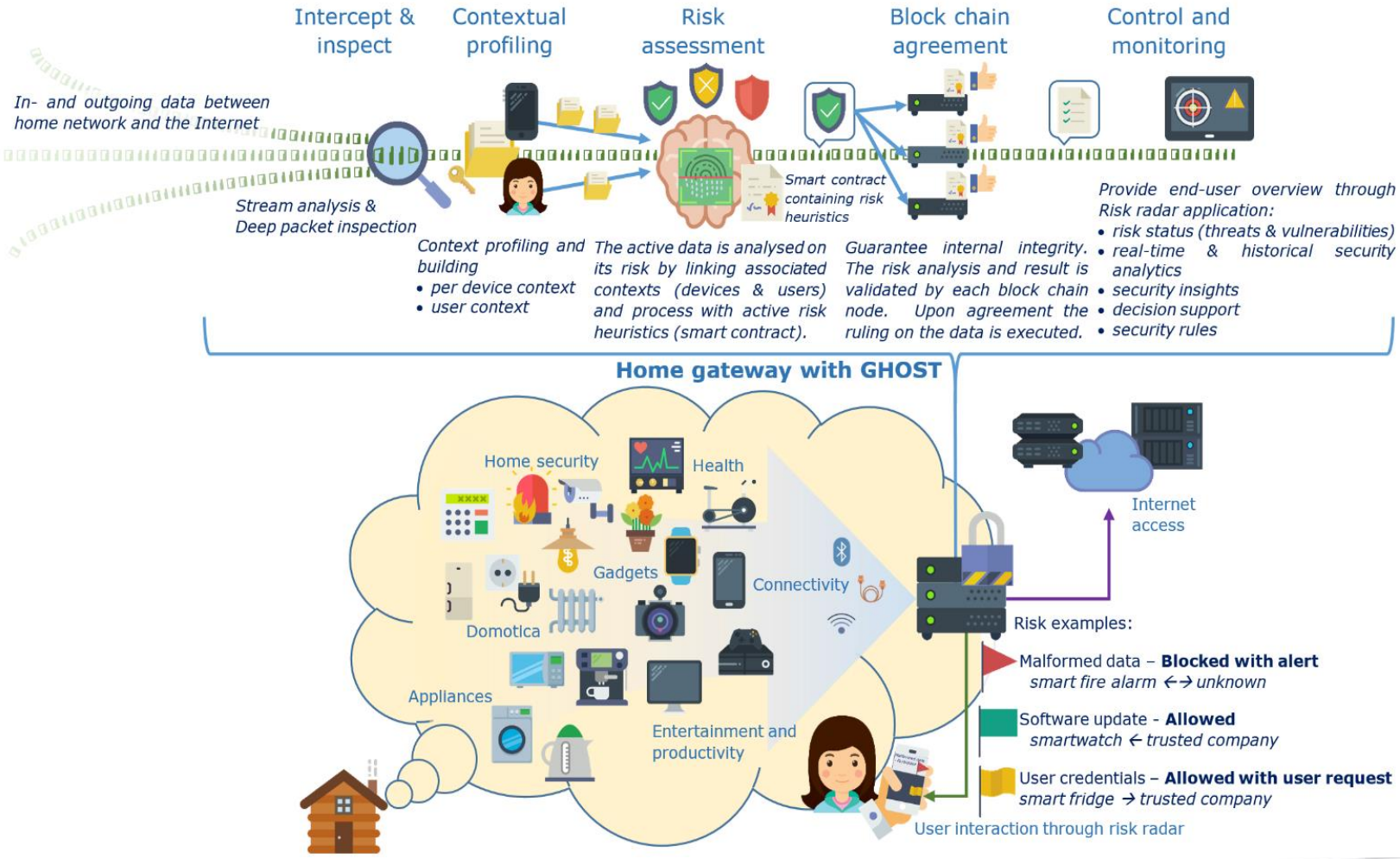
GHOST Key characteristics

- ✓ Generic, hardware agnostic, security solution for smart-homes
- ✓ Multiple different (wireless) protocols
- ✓ Network monitoring and anomaly detection approach
- ✓ Automatically handling the security incidents with minimum user intervention
- ✓ Usability of the interface for user interaction
- ✓ Running on limited hardware resources

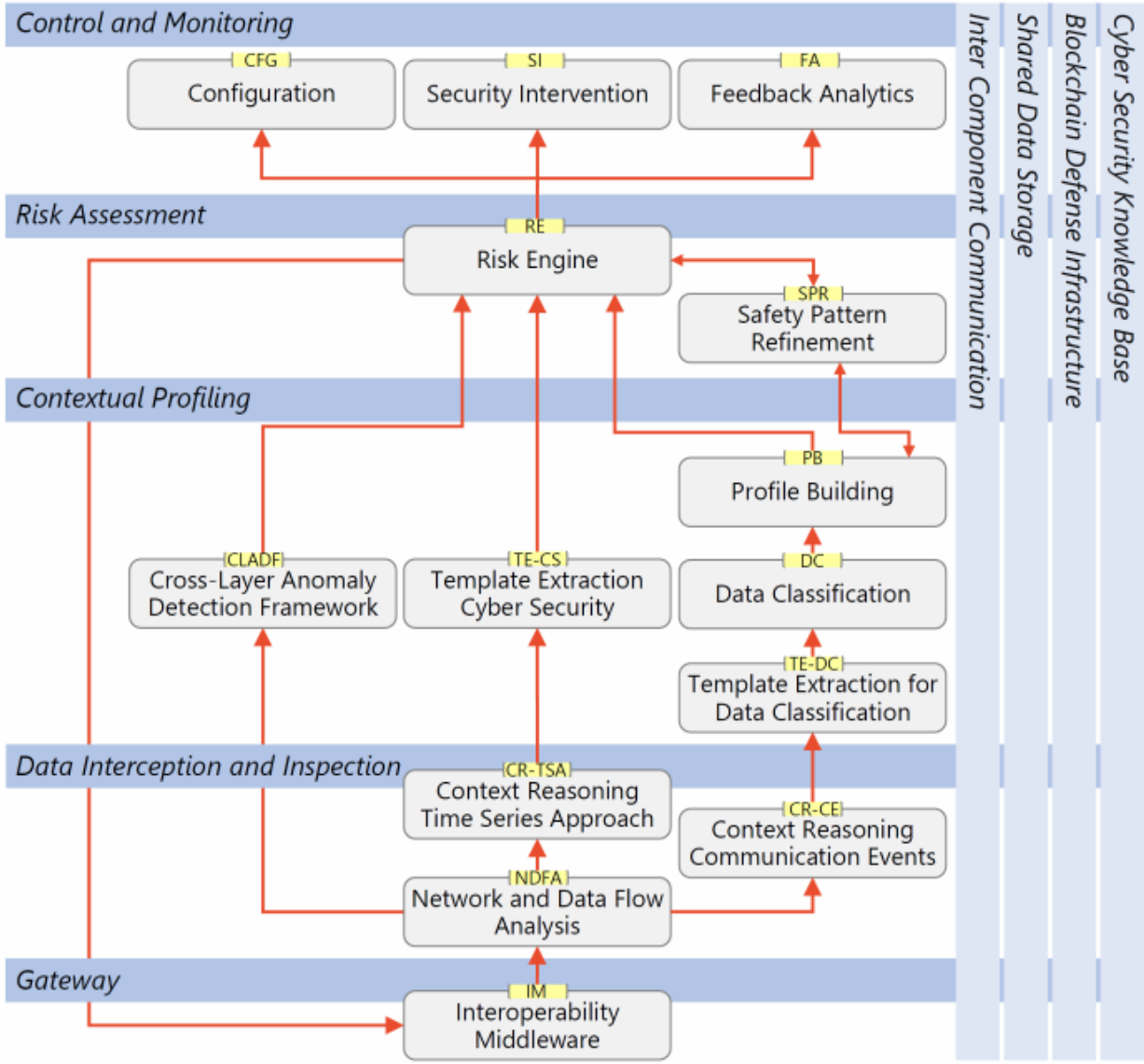
GHOST key aspects

- Use of the **state of the art technologies**
  - Machine Learning
  - Blockchain
  - …
- Focus on **usability** and **end user engagement**
  - End user as one of the weakest points of a security solution
  - Focus groups
  - Real Life Trials
- **Device-agnostic solution** but…
  - Software-based suite
  - Enhanced hardware capabilities
- **Academic-industrial balance** in the consortium
  - Orientation to the market

GHOST high-level concept



GHOST technical architecture



Data interception and Inspection:
Data gathering and extraction from network traffic

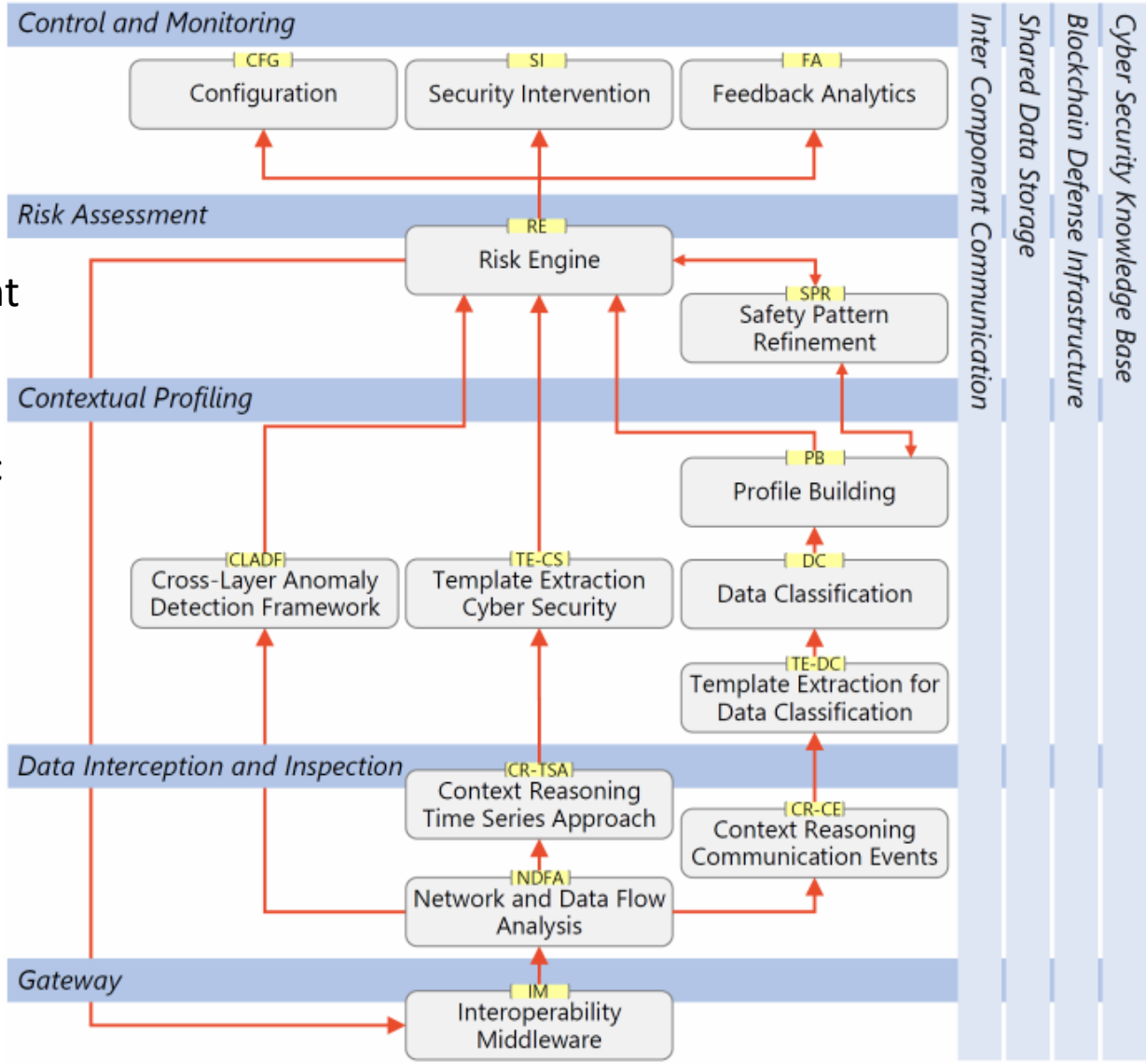
Gateway: Links the existing gateway with GHOST solution

GHOST technical architecture

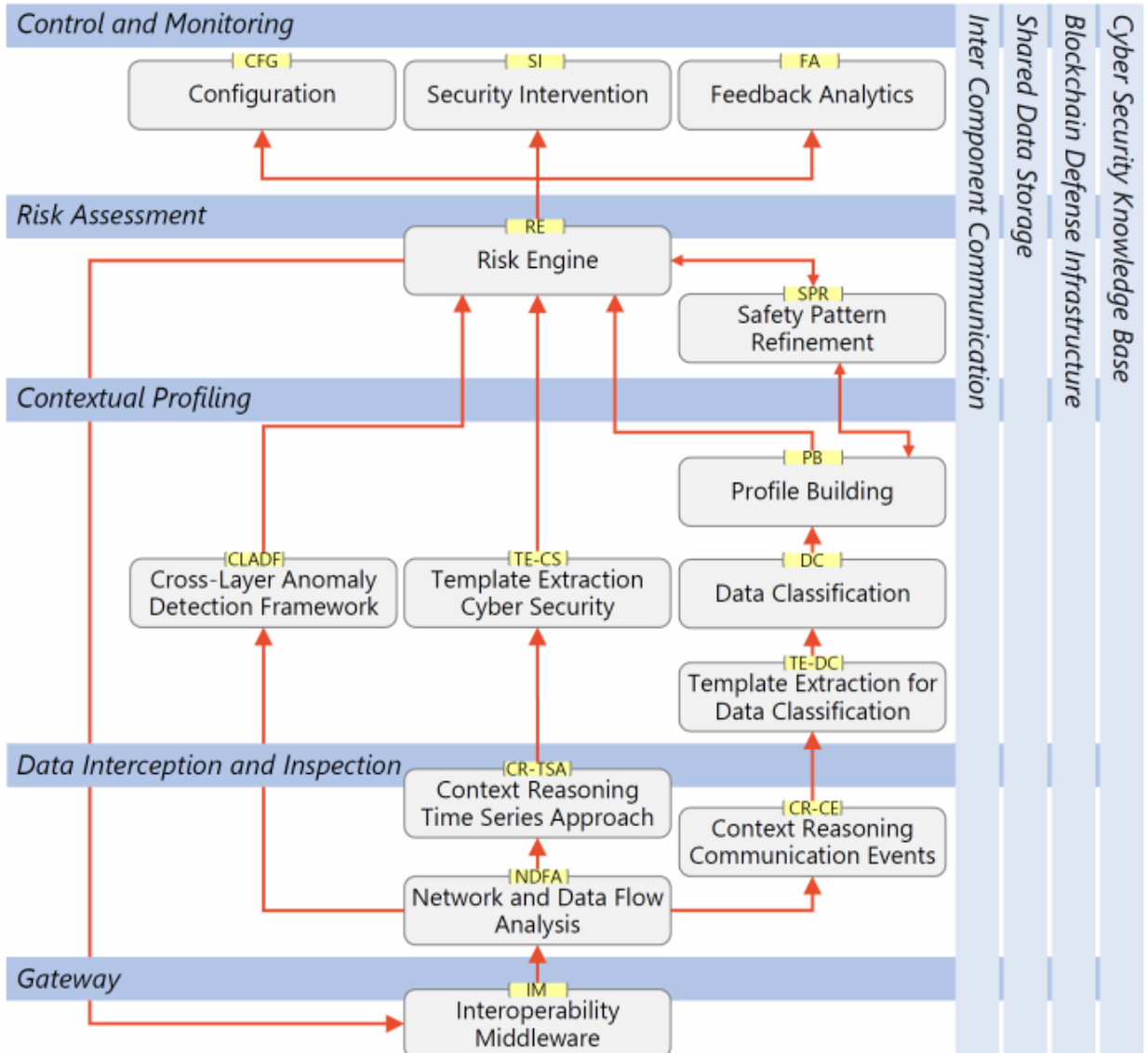
Control and Monitoring:
Visual friendly interaction with the user

Risk Assessment:
Receives intelligence report and performs real-time assessment

Contextual Profiling:
Extracts behavior of IoT devices based on the network traffic



GHOST technical architecture



Blockchain Defense Infrastructure:

Public blacklisting, forms of consent, software integrity

Challenges

- Heterogeneous wireless protocols
  - IP (Wifi)
  - Bluetooth
  - ZigBee
  - Z-Wave
  - RF869
- Limited Hardware Resources
  - Gateways with limited CPU and RAM capabilities

Safe-Guarding Home IoT Environments with Personalized Real-time Risk Control

Follow us on the Social Media

GHOST Project EU | GHOST Project EU | @GHOST Project EU | GHOST H2020 Project

More info in www.ghost-iot.eu

Thank you!