This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Workshop on Blockchain Applications to Industrial IoT

Cognitive Routing and Security Enhancement in the SerIoT

Sławomir Nowak
s.nowak@iitis.pl

IoT Week

Aarhus, 2019

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

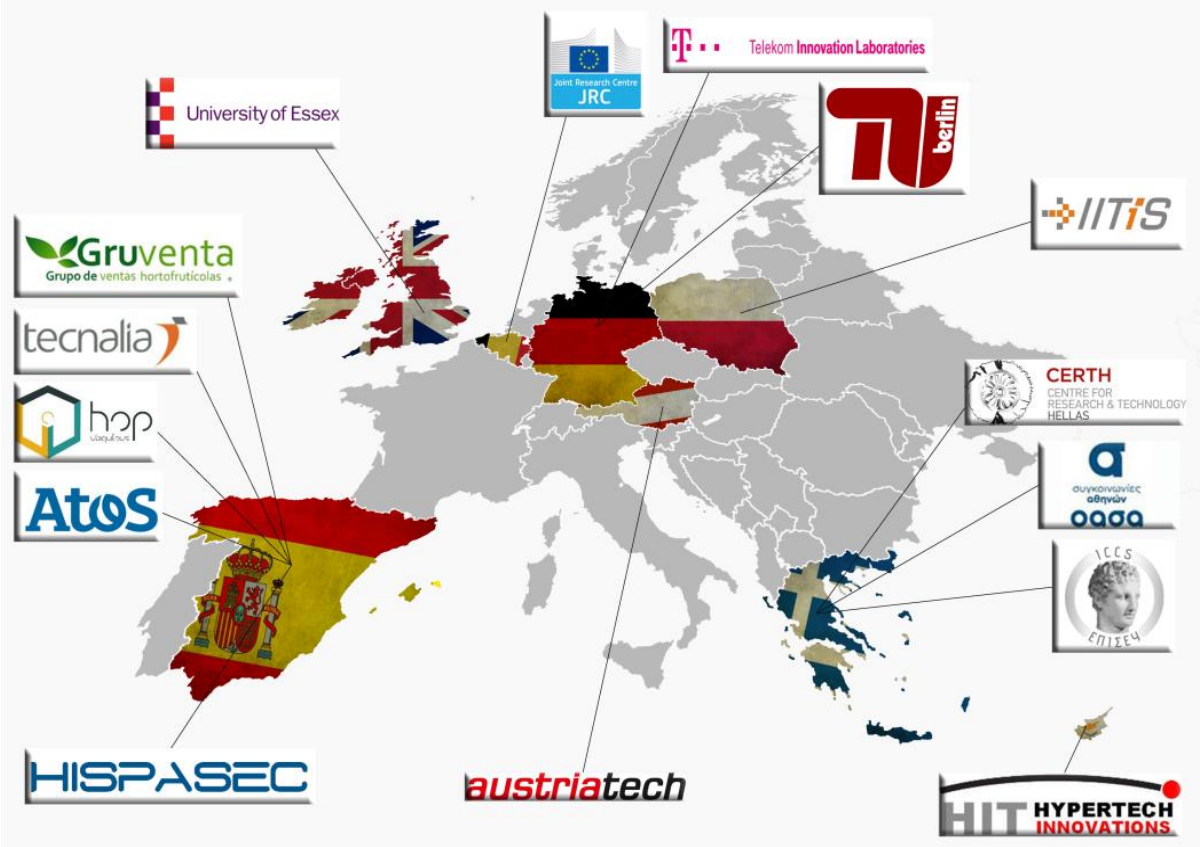
The Consortium

15 Partners:

- **Technological companies**
- **Research organisations**
- **Universities**
- **SMEs**

8 European countries:

- **Austria**
- **Belgium**
- **Cyprus**
- **Germany**
- **Greece**
- **Poland**
- **UK**
- **Spain**



This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Objectives

- **IoT a Secure, QoS and Energy Aware Routing of Information**
- **Real-time monitoring** of traffic exchanged by heterogeneous IoT platforms
- **Analytics Platform** to recognize suspicious patterns, detect threats and abnormal events
- **Honeypots to attract malicious attacks**
- **Policy-based framework** for usage control flow policies for end-to-end security & privacy
- **Socially, Technologically and Commercially significant Use-Cases** from different application domains
- **Commercially Viable Outputs** and **Business Plans**

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Application context

The results will be verified based on several **practical use cases**:

- **Surveillance**: security of multimedia data streaming from surveillance networks
- **ITS in Smart Cities**: security in Intelligent Transport Systems environment
- **Flexible Manufacturing**: enable a secure connected industry
- **Food Chain**: ensure end-to-end security along the food chain

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

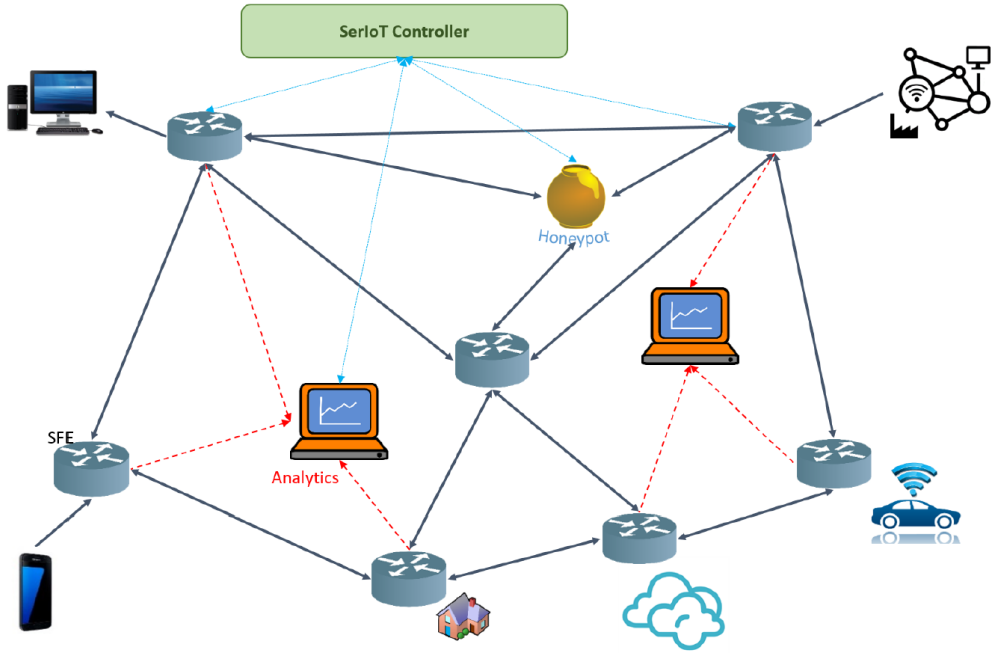
SerIoT approach

SerIoT Cognitive Packet Network interconnects distributed IoT subsystems and components

Software Defined Networks (SDN) + **Cognitive Packet Network** (CPN)

Smart Packets (SP) to search for **secure multi-hop routes** having good **quality of service**, considering also **energy efficiency**.

Random Neural Networks will be used as the routing decision engine.



This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Security Aware Routing

Software Defined Network
- Modern network management
- Centralized approach to flow control
- Data plane & control plane separated
- Convenient for IoT-aware infrastructure

Cognitive Packet Network
- Self Aware Network concept
- Cognitive Packets recognizing the state of the network
- Distributed optimization of network paths

SerCPN
- Effective security aware routing
- QoA and Energy awareness (secondary metrics)
- Supporting IoT-dedicated Fog substrate

Random Neural Networks as decision engine
Blockchain Ethereum as reliable storage

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Approach

SerCPN – the network for distributed IoT subsystems

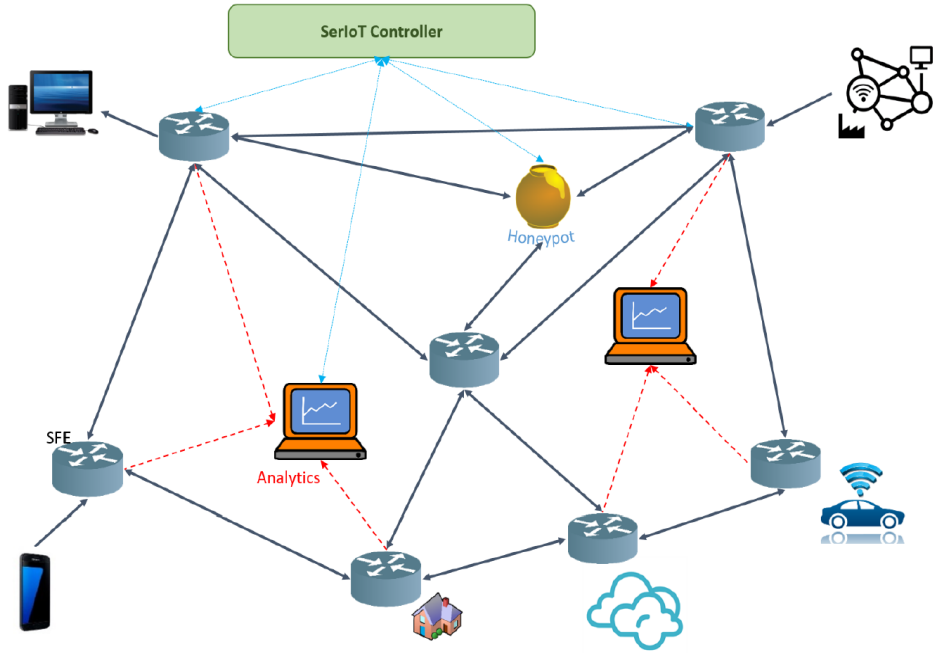
Cognitive Packets (CP) to search for

(A) secure multi-hop routes,

(B) quality of service,

(C) energy efficiency and **privacy constraints** considered

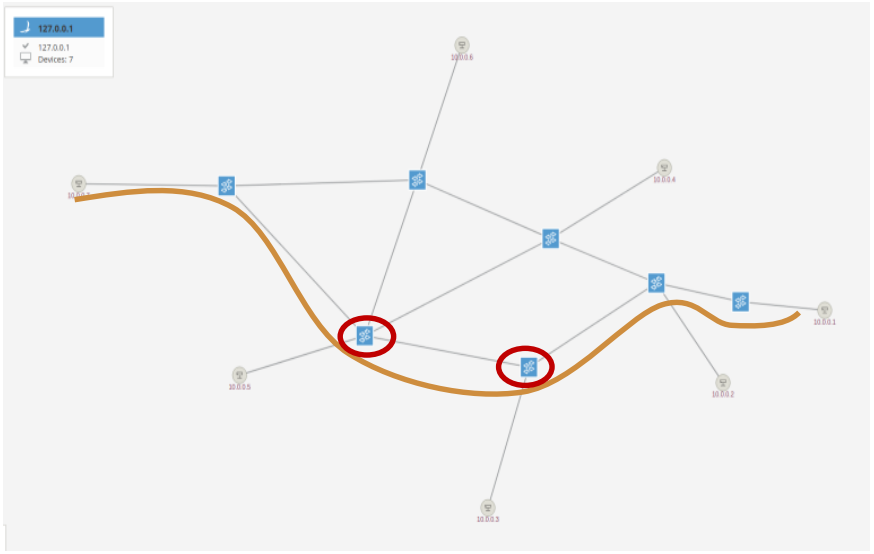
Random Neural Networks (RNNs)/ Reinforcement Learning for routing decisions.

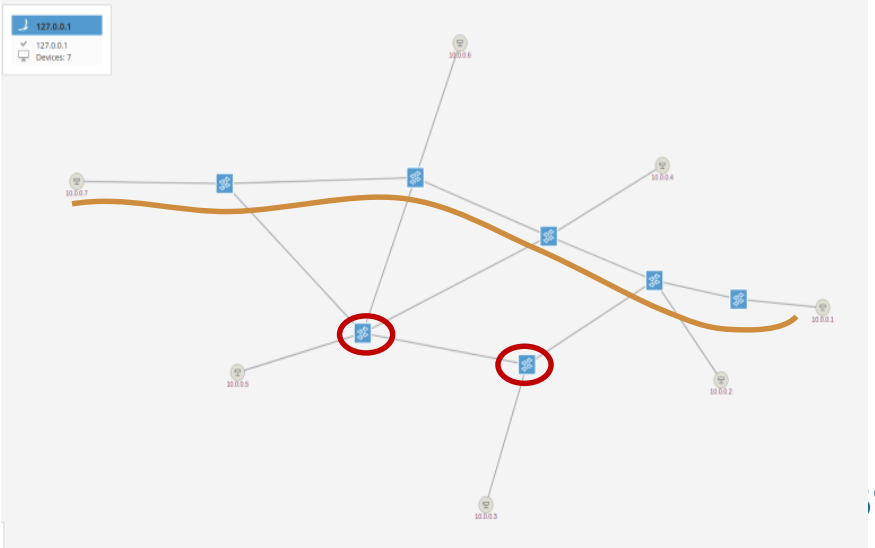


This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Security aware routing

- Full trust – QoS routing enabled
- No trust – perform mitigation decision
- **Limited trust (>0%, <100%)**
  - **introduce Security Aware Routing policies**
  - **redirect traffic through AD module**
  - **gain time for final decision, network elements/flows are protected also in the meantime**





This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Blockchain in SerIoT

Vision *"to provide a decentralized approach (...) using the latest breakthrough technology: Blockchain„*

"To research and analyse how can Blockchain contribute to improving IoT solutions. Moreover, to understand how to solve the know issues o IoT and blockchain"

"To explore introduction of Blockchain as a security and privacy preserving layer for IoT"

…but we don't have dedicated task or workpackages

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

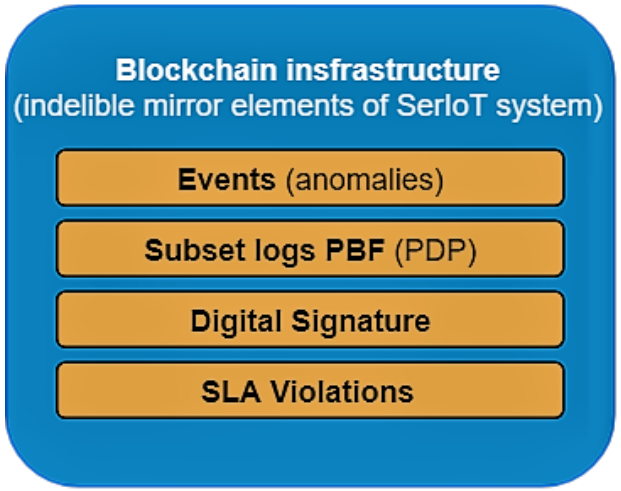
Opportunities of Blockchain

- Interoperability of IoT systems – heterohenious IoT data stored in blockchains
- Security – by securing data in blockchain
- Traceability of IoT data – providing traceable services
- Autonomic interactions – autonomous devices based on smart contracts

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Different SerIoT use cases

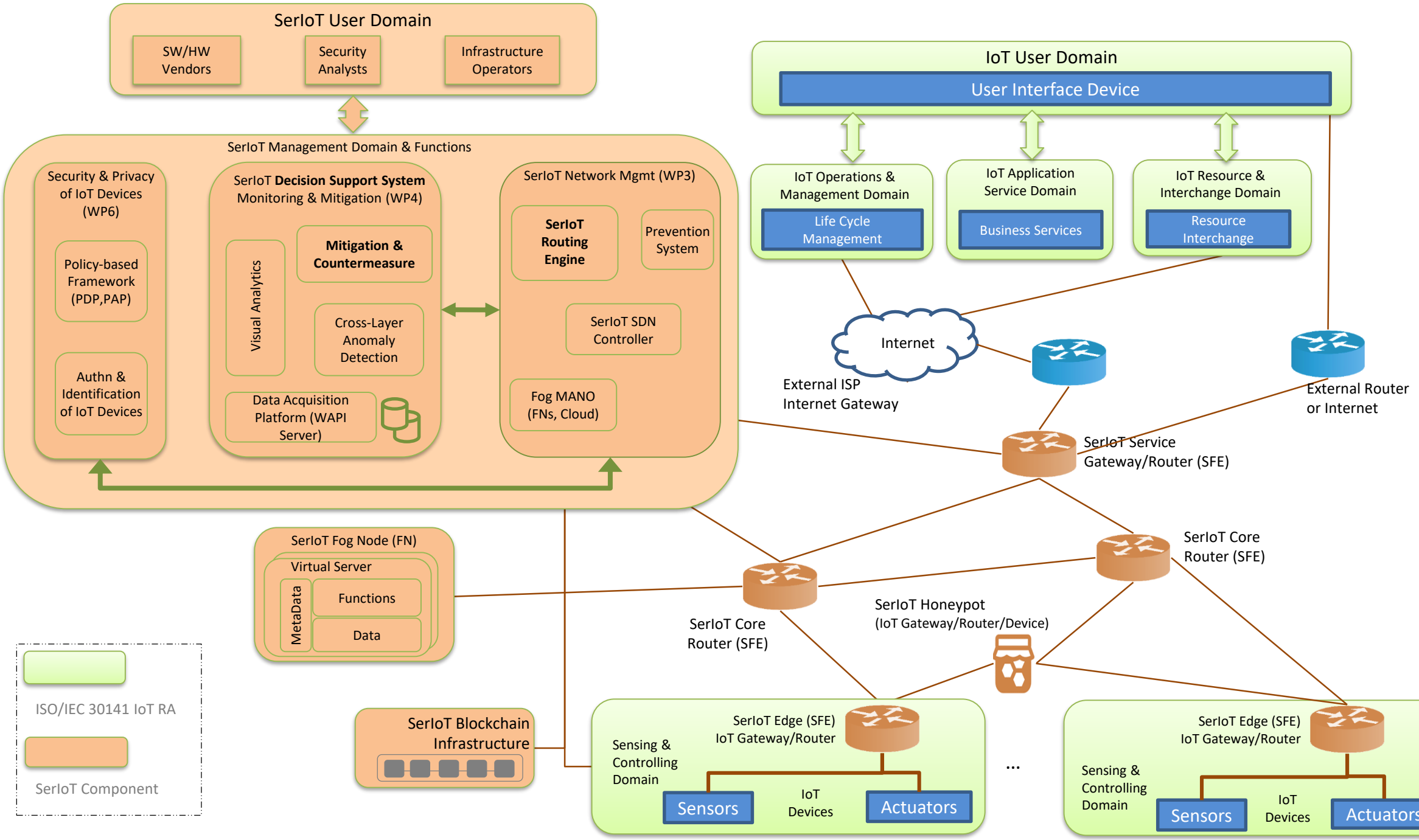
- **Events (anomalies)**
  - Erroneous authentication
  - Excessive requests per second
  - Excessive response times
- **Subset logs PBF (PDP)**
  - Policy Violations
  - Deny a user access to a specific database
- **Digital signature**
  - PSRAM - PUFs
  - Noise of sensors
  - Hash (MD5) from Software components
- **SLA Violations**
  - Parameter values of sensors out of range, e.g. temperature under threshold



This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Challenges of Blockchain

- Resource constrains – …to make device a full node ~180GB needed
- Security vulnerability – smart contracts defects, unstable technologies
- Privacy leakage – traceability of transactions
- Transaction cost – security costs
- Scalability – low throughput of transactions for public blockchains



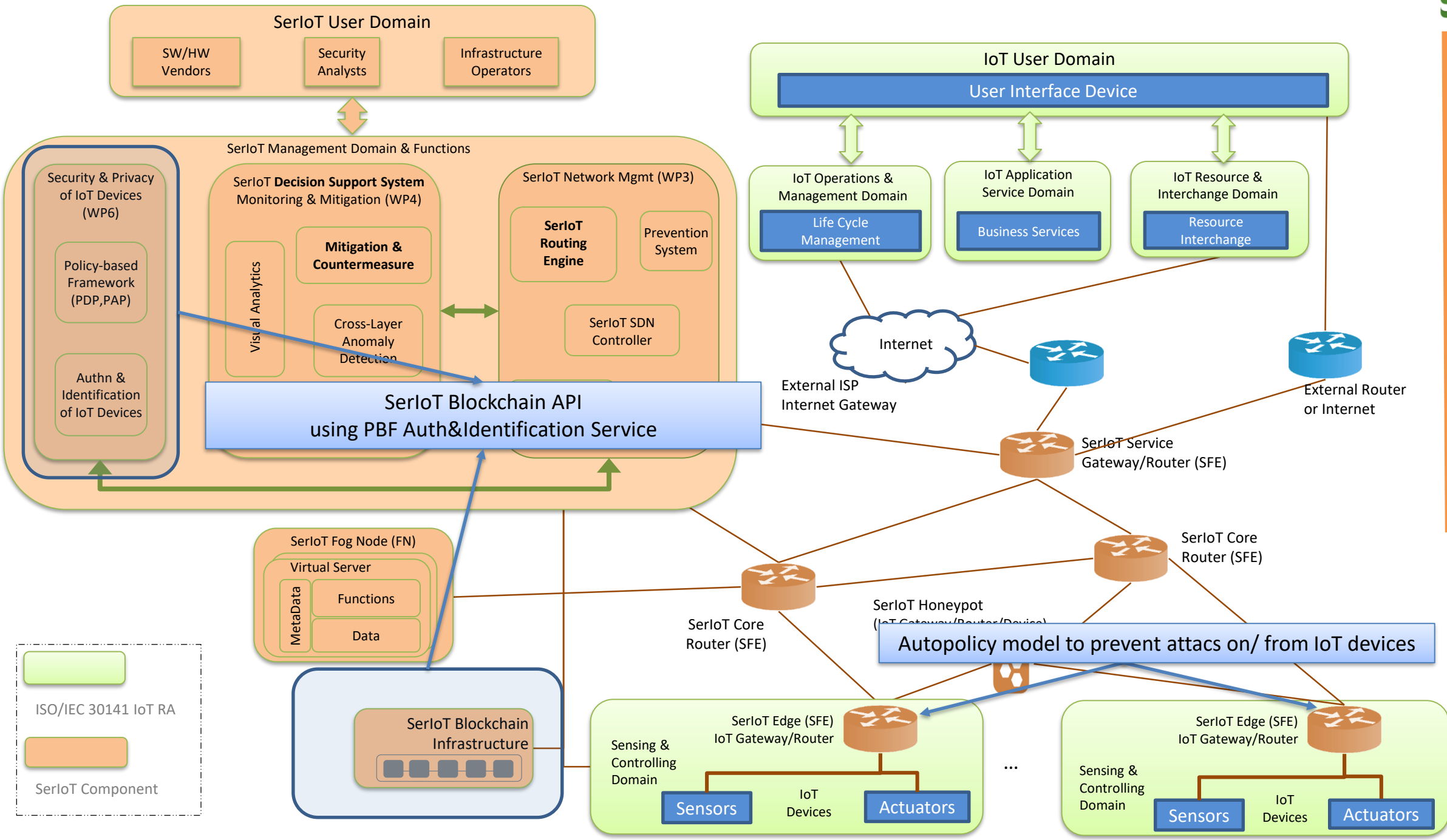
SerIoT network architecture

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Approaches

- Blockchain Policy Based API
- Public database of traffic profiles, to suport the Autopolicy model
- *Enhance the Cooperative Intelligent Transport System (C-ITS) improving the implementation of the revocation mechanism using Blockchain*

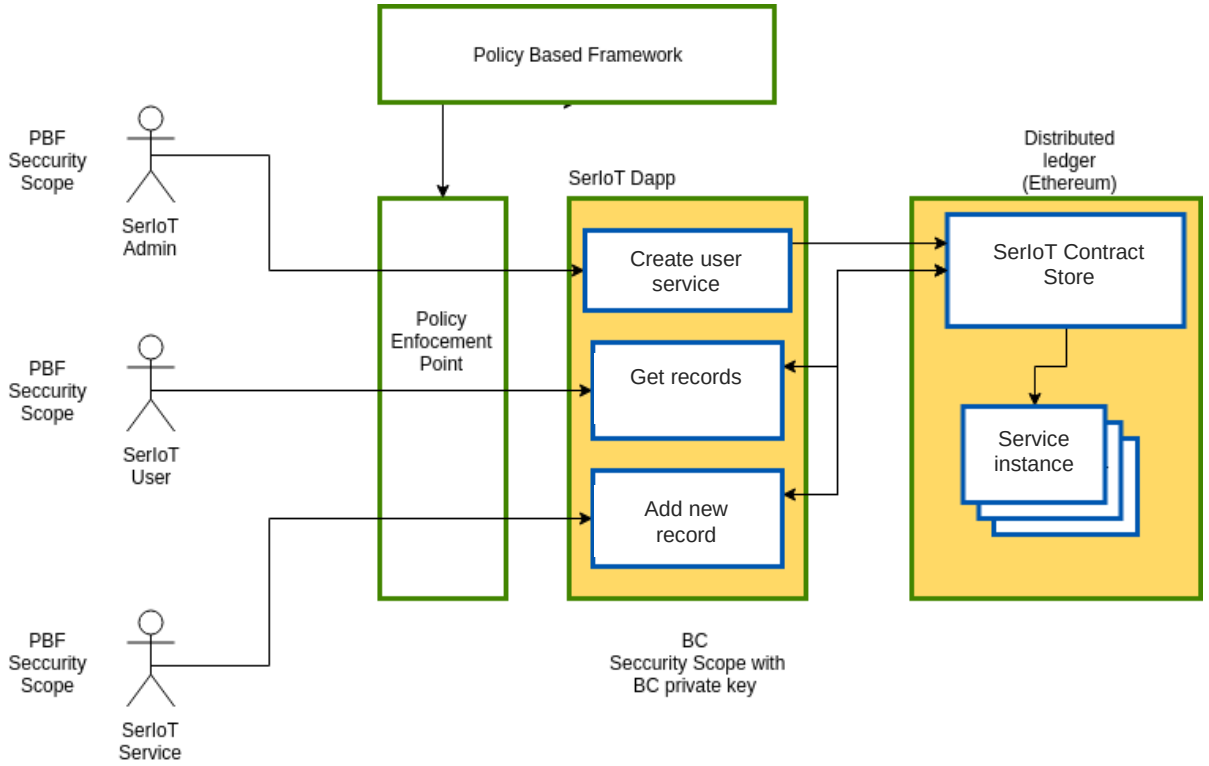
SerIoT network architecture



This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Blockchain Use Cases in SerIoT

General SerIoT Blockchain API



Authorization decision for the component or service requested

Actors:

SerIoT Admin
SerIoT Client
SerIoT Service

Services:

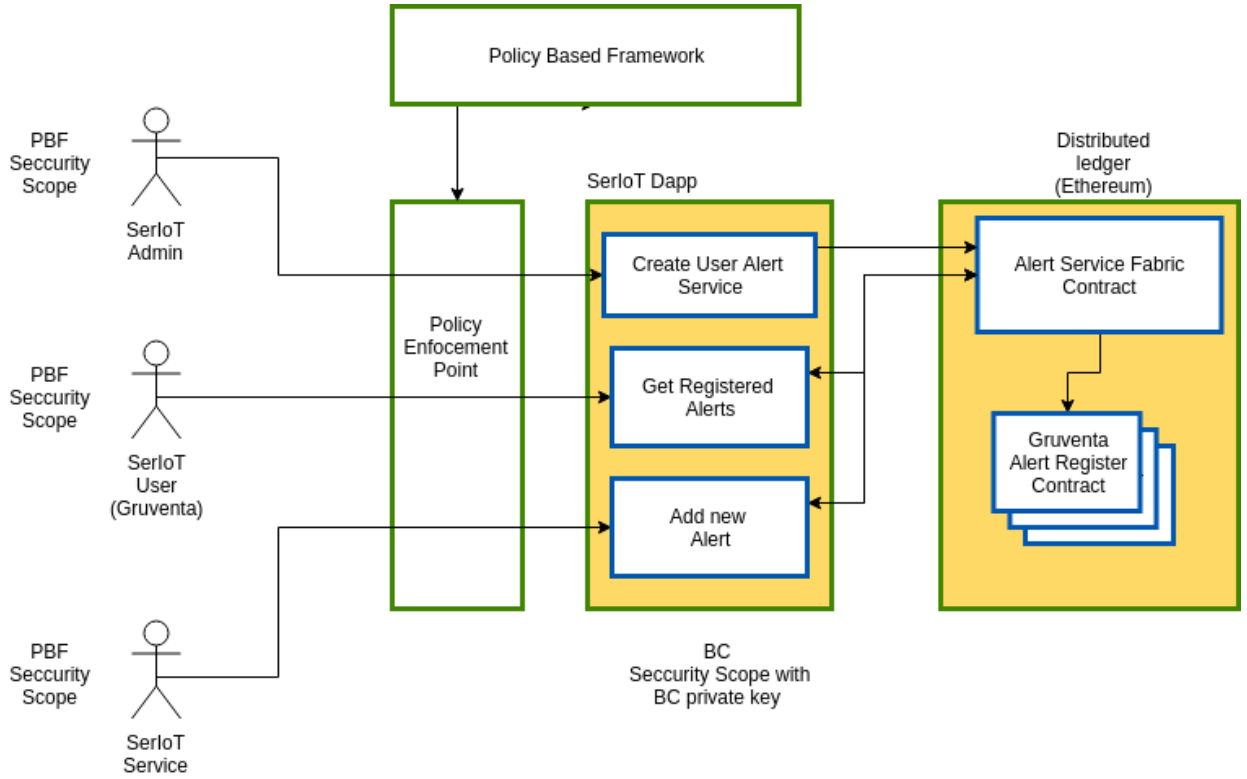
PBF Police Base Framework SerIoT Service
PBF BC Admin API Extension
PEP Policy Enforcement Point
Distributed Ledger Client

FIWARE Keyrock as IdM and PAP,
AuthzForce as PDP and FIWARE
Wilma PEP

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Alert register service

Alert Register Contract: implementation of a contract that stores the alert sent by the SerIoT Services.



Gruventa

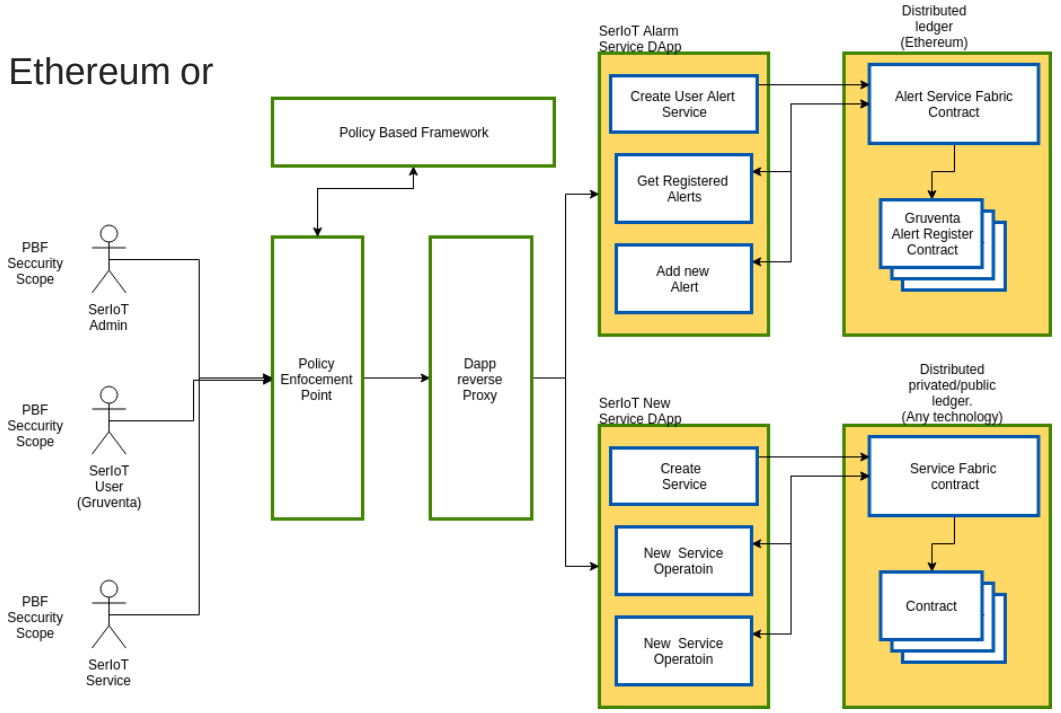
fruit and vegetable trading company

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

SerIoT BC Solution Extensibility

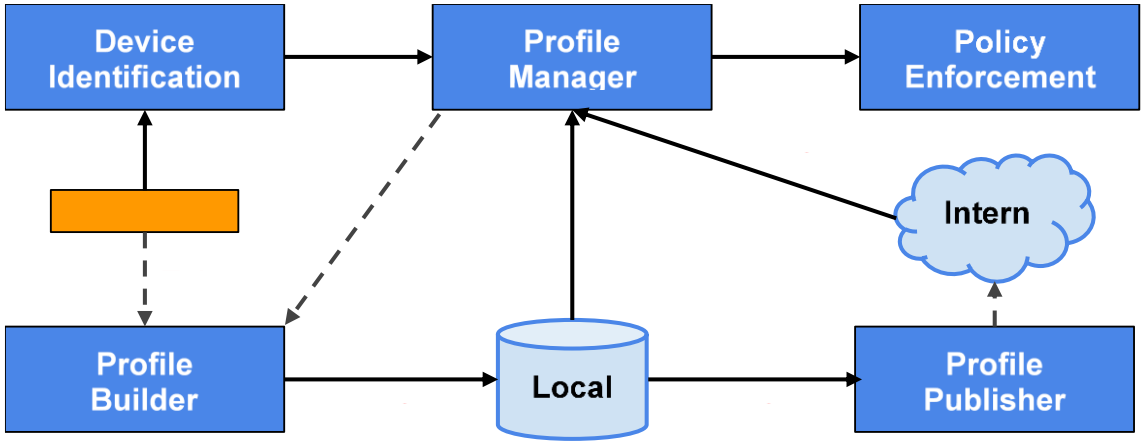
Towards universal solution to address different user level and system level use cases…

- ✓ PBF PEP and Dapp reverse proxy allow us to add new services
- ✓ Dapp reverse proxy allow us to use different BC technologies like Ethereum or EOS even introduce a private ledge for specific services.
- ✓ PBF allow us to share deny and access policy control through different BC technologies.
- ✓ Stateless Dapp allow horizontal scalability
- ✓ Dapp interfaces allow users and services to use the ledge in a easy way
- ✓ New actors, roles, attributes and policies can be introduced in a easy way



This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

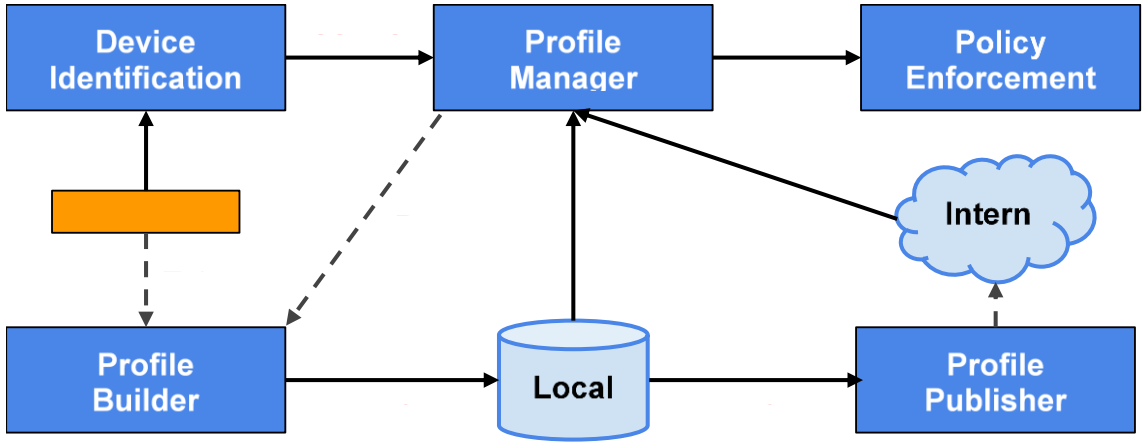
Autopolicy - a new IoT security model



- IoT device connects to the network
- Device Identification authenticates the device, by discovering its Identity
- Profile Manager finds its Traffic Profile
- The profile is sent to the Policy Enforcement function, which goal is to allow the flow but only under a set of strict rules defined by the profile

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Autopolicy - a new IoT security model



- requires each device to assign a traffic profile of the of machine-generated traffic e.g. maximum consumed bandwidth, set of contacted IP addresses
- automatic
- applies primarily to upstream traffic
- can significantly reduce the size of potential DDoS attacks
- takes advantage of the specyfic features of machine-generated traffic

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

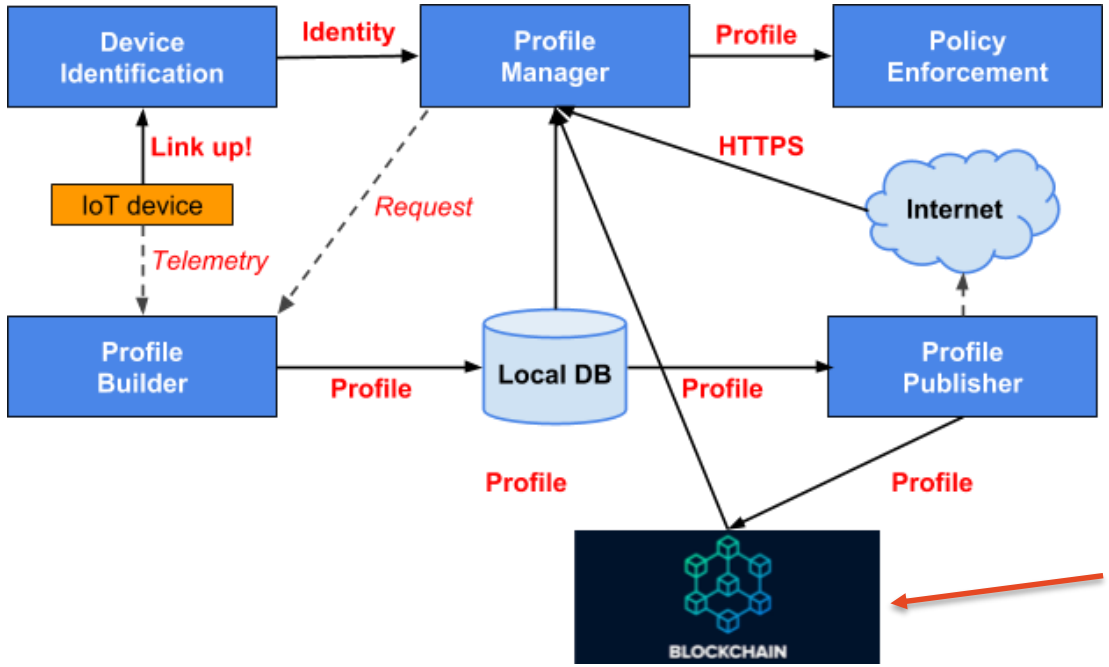
Autopolicy - a new IoT security model

Public database of profiles

- A shared, public database is needed
- Multiple writers (trusted/ untrasted) assumed
- Fully distributed service (no need of third party)
- Transaction in the database are related

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

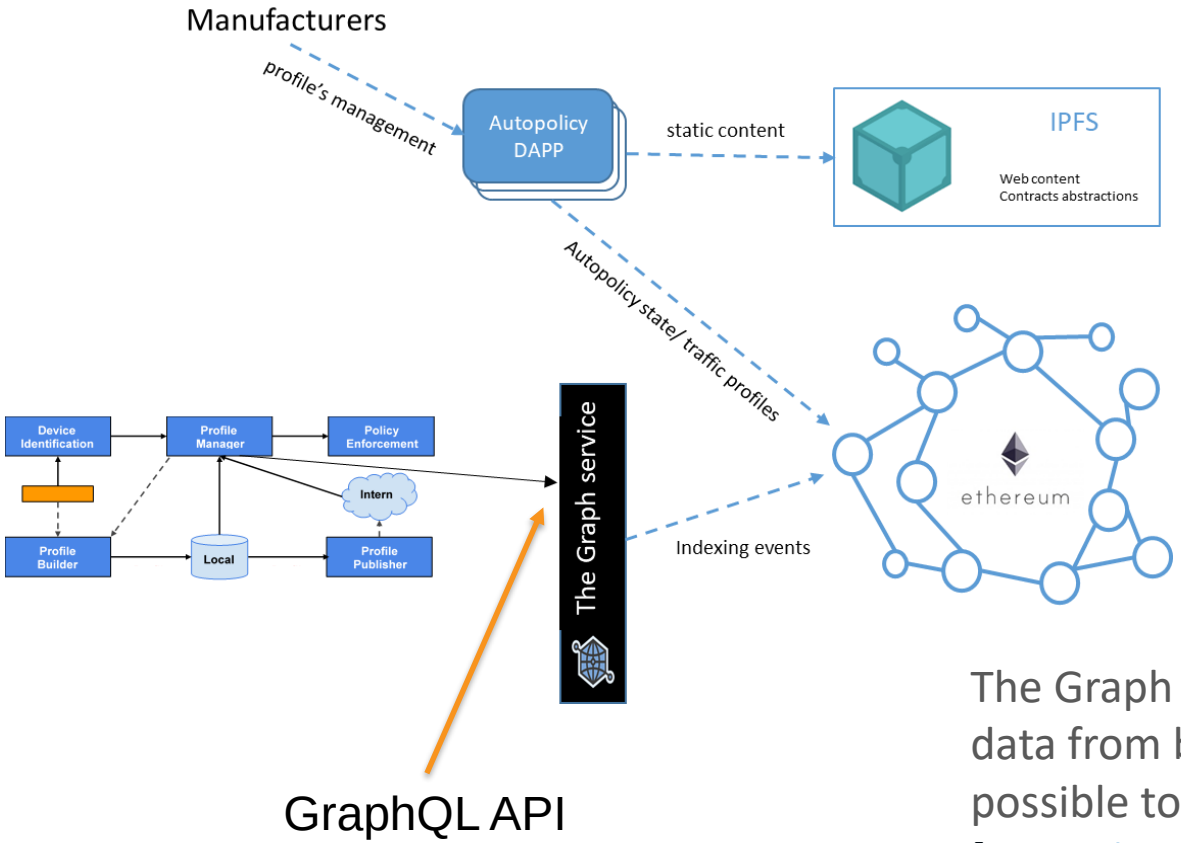
Autopolicy - a new IoT security model



How to query blockchain?

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Autopolicy - a new IoT security model

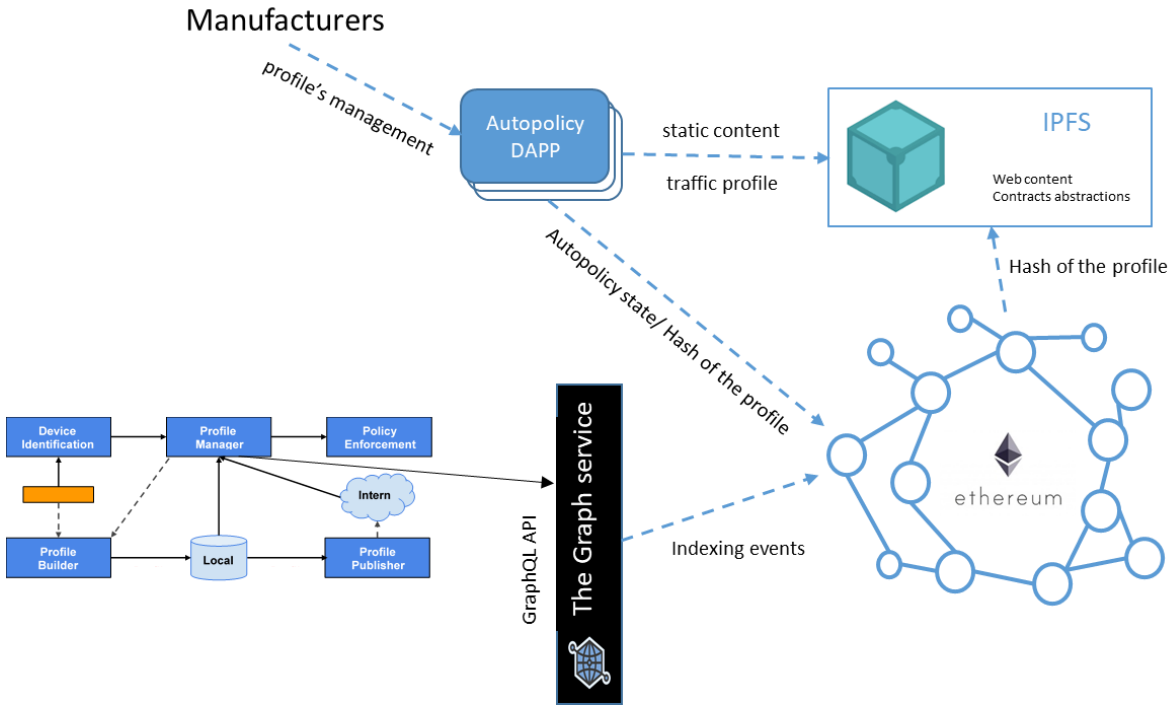


- The distributed architecture
- GraphQL interface used
- The Graph service for to query data in blockchain
- IPFS system to deal with the deploy the distributed WebService.

The Graph is a decentralized protocol for indexing and querying data from blockchains, starting with Ethereum. It makes it possible to query data that is difficult to query directly [www.thegraph.com]

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Autopolicy - a new IoT security model



- The of data records stored in distributed file system
- Enables more complex and larg data structure

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Remarks

- ✓ Blockchain may be useful, but not a „killer app" for IoT yet
  - ✓ Only simple, non critical solution accepted
  - ✓ Blockchain as backup, optional solution

A quote from one of our technical partners:

„…we consider blockchain as a method to make complex things even more complex…

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Q&A