From Hardware-Software Contracts to Industrial IoT-Cloud Blockchains for Security

Dimitris Bakoyiannis†, Othon Tomoutzoglou†, George Kornaros† and Marcello Coppola*

† Intelligent Systems & Computer Architecture Lab (ISCA-Lab)
Hellenic Mediterranean University, GR

*STM, Grenoble, FR
Outline

- Industrial IoT revolution for predictive maintenance, asset analytics, etc
- Convergence of IIoT, Cloud, LPWAN, Blockchain technologies
- Enhancing IoT devices, gateways security
- Integration of LoRaWAN infrastructure with Hyperledger Fabric
- Conclusions
Industrial IoT: Internet of Trust!
Security Risks in Connected IoT
IloT and Blockchain Convergence

- Blockchain: Smart contract enforcement
  - Decentralization (identity management, access control)
  - Tamper-proof data (immutable, traceable, signed-timestamps)
  - Information security (confidentiality, integrity)
  - Privacy (disassociate public keys/hashes from user IDs)
Enhancing Device Security

**User Data**
- Timestamp
- Source/Destination
- Product Data (ID, S/n, Attributes, Exp Date)

**Read-Only Data**
- Unique Tag-ID
- UID Signature
- Tamper Status

**Devices**
- Dx
- Dx
- Dx
- Dx

**Gateways**
- Long-range Sub-GHz LoRa®
- 3G / 4G / Ethernet (IP)

**Network Servers**

**Application Servers**
Etherean (IP)
Secure Gateway via Trusted Devices

- Trusted boot-chain
- Trusted Execution Environment

Gateway Security

STM32MP1-DK2
Authority Verification of End-Device

1. **Manufacturer**
   - TRUST25

2. **RFID/NFC**
   - Private Key
   - Device Unique ID
   - Application ID
   - Public Key

3. **MCU**
   - LoRa

4. **IoT Node**
   - Request IoT node identification
   - Provide Certificate
   - Send Challenge
   - Digitally sign Challenge with Private Key
   - Send Signature
   - Verify IoT Node Signature

5. **Originality Verifier**
   - Certificate Authority (CA)
   - Public Key
   - Verify IoT Node Certificate
Isthmos Bridging/Proxy Service

- LoRaWAN and Fabric bridging to store IoT data to the Ledger
- API for other services to monitor and control Ledger operations
- Integrated features
  - Fabric SDK client to:
    - Register/enroll with the Fabric certificate authority (CA)
    - Interact with the Ledger to read/store data
    - Register for fabric events
  - MQTT client to:
    - Receive LoRa uplink messages to forward to Fabric
    - Forward downlink data (e.g., control commands) to LoRa IoT devices
  - HTTP server to allow monitoring services (e.g., Prometheus, Grafana)
Integrated LoRaWAN and Hyperledger Fabric

![Diagram of LoRaWAN and Hyperledger Fabric integration]

- LoRaWAN App Server
- LoRaWAN Gateway
- Isthmos
- MQTT Client
- Fabric Client
- HTTP Server
- Fabric Network
- Fabric Peer(s)
- Ledger
- Prometheus/Grafana

LoRa IIoT Device Enhanced with NFC/RFID

LoRaWAN network diagram showing integration with Hyperledger Fabric.
Use Cases

▪ Automation Monitoring and Maintenance in Manufacturing
  ▪ Access and manage IoT devices/data in an industrial environment (IIoT)
    ▪ Trusted monitoring of IoT device data (e.g., sensor values) at the ledger
  ▪ Management of IIoT device lifecycle by using firmware updates
    ▪ Record update information metadata at the ledger that can be used to manage the firmware update procedure of IoT devices
Industrial Monitoring (power, gas)
FOTA Updating

- Director Server
  - send FW metadata
  - receive FW metadata
  - OR
  - Blockchain

- FW IMG
  - FW Metadata
  - send FW metadata
  - receive FW metadata

- OEM Gateway
  - GIT push
  - FW IMG
  - FW Metadata

- GIT Server
  - GIT push
  - GIT pull

- Island Gateway
  - EndPoints 1
    - EndPoint 1
    - FW IMG
    - FW Metadata

- Island Gateway
  - EndPoints N
    - EndPoint N
    - FW IMG
    - FW Metadata
Different Fabric network configurations based on the number of organizations, peers and channels

Benchmark client application per peer invokes 2000 transactions sequentially for each available channel
Summary

- A combination of IoT device authentication via hardware/software methods and decentralized integrity assurance framework
- Isthmos secure bridging of IoT data over LoRaWAN with Hyperledger Fabric
- Investigation on performance and scalability when partitioning Fabric Ledgers in the scope of different channels
Thank you for your attention!

EU-H2020 AVANGARD

Intelligent Systems and Computer Architecture Lab
https://isca.hmu.gr

George Kornaros
[kornaros@hmu.gr]