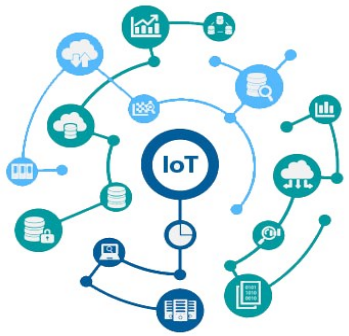


CHARIOT – 3rd Workshop

Wednesday 22 October 2020 (online)

IoT Data Security and Privacy Solutions – Challenges and Opportunities for Airports

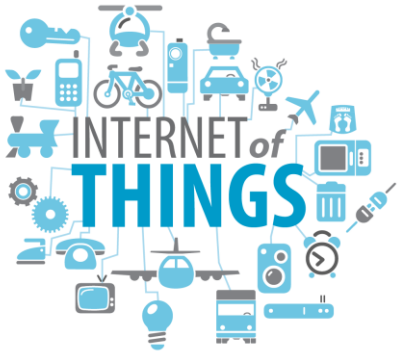
Blockchain as an enabler in the CHARIOT Integrated approach to Industrial IoT Safety, Privacy and Security

Konstantinos Loupos,
MEng, MSc, PMP, MBA

Head of R&D Program
INLECOM

Cognitive Heterogeneous Architecture for Industrial IoT
"CHARIOT"

Topic:	IoT-03-2017 - R&I on IoT integration and platforms
Type of Action:	Research and Innovation (RIA)
Funding:	4,928,562.50 €
Duration:	36 months
Start Date:	1/1/2018



CHARIOT Objectives and Scope

- CHARIOT's central focus is **Industrial Systems (industrial IoT)**
- Systems whose **failure or malfunction can result in harm, injury or death, loss or damage to property, or impact to the environment**
- Comprise H/W, S/W, infrastructure, networks and human **aspects needed to perform safety functions**, where failure would cause a significant increase in the safety risk for the people or environment
- **Securing data, objects, networks, infrastructure, systems & people in IoT** will have a prominent role in the research and standardization activities over the next several years
- CHARIOT also recognises that **security threats are broad, and have the potential to compromise IoT systems or alter their intended operation**

CHARIOT - Offerings

IoT Devices' Lifecycle management

- Blockchain-based PKI for sensor and gateway authentication
- Blockchain-aided encryption between all IoT network endpoints (sensor/gateway/FOG)
- Mobile application for sensor provisioning in the IoT network utilizing the four-eye principle
- Blockchain-based state management for sensors (decommissioned, faulty, compromised etc.)

IoT Firmware Development and Deployment

- Securing firmware through rule-based code analysis and injection of analysis results & the source code hash within the binary code
- Security Engine: filter firmware based on rules applied on the injected analysis results
- Security Engine: processes firmware binaries and identifies security vulnerabilities (e.g. code injection) by cross-referencing historical software updates and vulnerability databases
- Extraction of the injected firmware hash and version and validation with the blockchain at the gateway level

Intelligent IoT Data Analytics and IPSE

- Privacy Engine: ensures privacy by design by handling the data encryption policies based on blockchain technologies to avoid privacy breaches in the IoT network
- Privacy Engine: detects sensitive data streams through analysis of the sensor data
- Safety Supervision Engine: Machine learning anomaly detection based on user-defined models and neural networks (e.g. LSTM)
- Safety Supervision Engine: IoTL to manage the dynamic network configuration, describe access control rules and define the network topology
- Predictive Analytics: Use predictive analytics algorithms and analytics processing tools to highlight out-of-bounds behaviours and assess combined interdependent risks

Platform and User Interfaces

- CHARIOT Platform core: orchestrating mechanism for sensor data ingestion, management, storage, normalization and external connectivity API
- CHARIOT Platform core: managing machine learning models training on the cloud and fog utilization
- Device Management Dashboard: handling blockchain devices registration, firmware updates and engine management as well as a user interface for the IoTL
- Operational Dashboard: providing Engines' health and performance monitoring as well as alerts' and sensor data visualization
- Agent-based simulator: to support IoT applications modelling and Privacy, Security, Safety Threat Vulnerability Analysis using multiple methods of assessment such as agent and network-based methods

Security Related Business Cases and Industrial Overview

NEEDS:

- In modern IoT configurations, **devices acknowledgement** is required as, a platform based, approach in commissioning, managing, tracking, securing and maintaining all network devices. This to provide:
  - **Productivity improvement –** via improved asset utilization enabling personnel focusing on core/value creation
  - **Reduced downtime** - via device management and real-time sensor/security monitoring -> service reliability
  - **Reaction to alerts** - steaming from network security issues - immediate issue identification and avoid of cascading effects
  - **Increased trust** of information from monitoring systems - creating network of sensors automatically authorized, commissioned, fault-approved reducing thus manual interventions
  - **End-to-end affirmed network components** - extended trust on the actual devices and conveyed information

CHARIOT BLOCKCHAIN-related OFFERING:

- End-to-end network solution with advanced capabilities for devices (sensors, gateways, etc.) authentication (via keys' embedding) combined with blockchain and encryption technologies.
  - **Combined authentication solution of blockchain with PKI** (Public Key Infrastructure) technologies in the actual network devices (sensors and gateways)
  - **Blockchain-aided encryption** between all IoT network endpoints (sensor/gateway/FOG)
  - **Mobile application for sensor provisioning** in the IoT network utilizing the four-eye principle
  - **Blockchain-based state management for sensors** (decommissioned, faulty, compromised etc.)
  - **CHARIOT sensors (WiFi & BLE)** with high processing capabilities (supporting encryption, blockchain etc.)

Sensor and Gateway Authentication

- Crucial requirement of any blockchain to **operate in an asynchronous fashion** (network-eccentric nature)
  - External module was required to be integrated in most industrial gateways

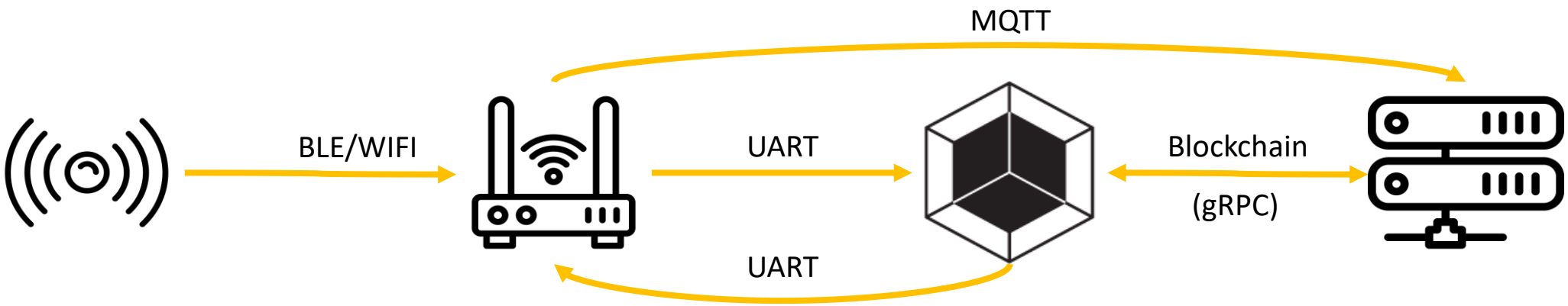
- **Industrial IoT gateways operate a real time operating system** in comparison to the traditional operating systems common household devices use, prohibiting a blockchain implementation from being deployed to one
  - Blockchain-capable modules called SoMs (System-on-Module) were correlated and the optimum module was discerned and ordered to be integrated within the CHARIOT gateway in correspondence with TCS

- **Selection and purchase of ARTIK device**
  - Integration of ARTIK on PANTHORA gateway
  - Setup of UART interface
  - Testing of communications and APIs

Sensor and Gateway Authentication

- **Blockchain Keypair**: A tool for generating the appropriate CHARIOT compliant keypairs for interacting with the CHARIOT blockchain
- **Blockchain Keypair API:** A RESTful API for generating the appropriate CHARIOT compliant keypairs for interacting with the CHARIOT blockchain
- **Blockchain Deployment:** Deployment scripts for properly initiating all services of the CHARIOT system, including the blockchain component
- **Distributed PKI Smart Contracts:** Smart contracts implementing the logic of a non-authoritarian PKI system using state-of-the-art cryptography, nonce-based systems & a pseudo-language for assessing instructions
- **ARM-based Blockchain Runtime:** A blockchain compilation of the Hyperledger Fabric suited for the ARMv8, or aarch64, architecture which hadn't been conducted in the past
- **Blockchain Service:** A RESTful API for interacting with the blockchain instance and generally handling all operations of the underlying smart contract

Sensor Authentication and Data Exchanges



CHARIOT IoT Sensor

- Produces Sensor Readings
- Retains a Cryptographic Keypair
- Implements End-to-End Cryptography

CHARIOT Gateway

- Relays Sensor Readings
- Handles FTP Software Updates
- Implements End-to-End Cryptography

Blockchain Module

- Maintains a copy of the Blockchain
- Validates Sensors
- Validates Software Updates

Fog Server

- Stores Readings in Database
- Enforces ACLs and protects privacy
- Enforces rule-based and ML-based policies
- Conducts Analytics
- Operates the rest of the CHARIOT services

Blockchain Encryption

- **Security Requirements** of IIoT communications are stringent:
  - IIoT devices themselves lack extensive computational capabilities
  - A high level of security bits is demanded
  - Near immunity against deciphering by non-negligible computational resources is expected

- **Current solutions** lack in several layers:
  - Susceptible to a wide range of attacks e.g. Single Point of Failure
  - Require supplementary infrastructure beyond the IoT network components e.g. Traditional PKI systems
  - Face difficulty in scaling across large IoT deployments

- **Blockchain** enters as mediator:
  - Enables devices themselves to act as part of the solution
  - Securely stores identification data of sensors along with status reports f.e. compromised
  - Segregates the network thus increasing its resilience and subsequent security
  - Inherently scalable as blockchain is so by design

Blockchain Encryption – Uses in CHARIOT

- **CHARIOT Blockchain Contribution:**
  - **Stores the hash of any software updates** that are to be relayed across the network, allowing their validation on each endpoint of the journey
  - **Stores metadata of the aforementioned software updates** aiding in the proper selection, categorization and cross-verification of a hash
  - **Stores the identities of any sensors** interacting in the CHARIOT network
  - **Stores their status along with attached metadata** that help in properly responding to communication requests by said sensors
  - **Stores the keypairs of CHARIOT services**, helping the Privacy Engine to properly encrypt messages across the various service endpoints of the CHARIOT network
  - **Stores the administrator accounts** of those responsible for maintaining the blockchain records
  - **Stores the enforcement policy** (n-out-of-m scheme) for each asset type (software, sensor, service, administrator)

Blockchain Encryption - Innovation

- Novel methodology via which **communications can be easily encrypted** with minimal computational resources whilst retaining a high level of security bits
  - Secure against any attack vectors that rely on brute-force attempts with non-negligible computational resources

- First applied at the communication's handshake, using identification information to asymmetrically calculate a **common cryptographic key between participants**
  - Utilizes the Diffie-Hellman Key Exchange (DHKE) over the prime256v1 Elliptic Curve (EC)

- **Actual communication encrypted** using the Advanced Encryption Standard (AES) algorithm in Cipher Block Chaining (CBC) mode
  - Initialization Vector (IV) exchanged during the handshake step ensuring atomic communications

Blockchain Encryption - Innovation

- Different approach applied to the handshake cryptographic algorithm.

- **To avoid duplicate keypairs, we instead introduced a dual-purpose to the existing keypair** used for the CHARIOT blockchain system
  - The keypair demanded by the CHARIOT blockchain is an Elliptic Curve keypair
  - Elliptic Curves do not restrict themselves to digital signature algorithms, they can also be applied in asymmetric cryptography
  - The Diffie-Hellman Key Exchange can be applied over an Elliptic Curve thanks to this property, thus allowing us to use the same keypair for both functionalities.

- An open-source implementation for the Elliptic Curve Diffie-Hellman Key Exchange was pinpointed
- Choosing open-source implementations instead of reinventing the wheel allowed us to take advantage of battle-tested, scrutinized and collectively devised code, thus ensuring that it is optimized to the greatest extent possible

Contact Details

INLECOM

Konstantinos Loupos, MBA, PMP, MEng, MSc

Konstantinos.loupos@inlecomsystems.com

The project CHARIOT has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780075