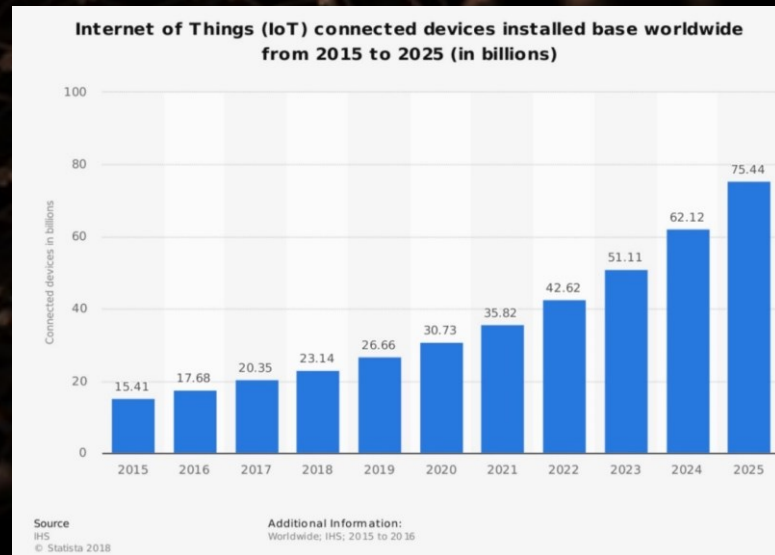


Integrated Solution for Industrial Data Security – The CHARIOT Solution

Konstantinos Loupos, MBA, PMP, MSc, Meng
Head of R&D program, INLECOM
(CHARIOT project coordinator)

Eclipse **SAM IoT 2020**
Security | AI | Modelling

- By 2025 it is anticipated that there will be **75 Billion IoT-connected devices Worldwide**
- **Spending on IoT devices and services reached \$2 trillion in 2017**, with China, North America, and Western Europe accounting for 67% of all devices (Gartner Inc)
- Growth in connected devices is anticipated accelerate due to a **rise in adoption of cross-industry devices** (LED lighting, HVAC systems, physical security systems and lots more)
- In recognition of this, **Secure IoT** is now becoming a more important focus of attention



- **Internet of Things (IoT) security breaches have been dominating headlines recently**
 - WikiLeaks's trove of CIA documents revealed that internet-connected televisions can be used to secretly record conversations
 - Trump's advisor (Kelly-Anne Conway) believes that microwave ovens can spy on us (through microwave cameras which can be used for surveillance)
- **96% of security professionals expect an increase in IoT breaches this year (Forbes 2017)**
- Recently, ISP Dyn came under attack – **cyber-criminals commandeered a large number of internet-connected devices** (mostly DVRs and cameras) to serve as their helpers
- Requests for government regulation of the IoT, asserting that **IoT manufacturers and customers are not paying attention to the security of IoT devices** (Bruce Schneier, Cybersecurity expert)



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's central focus is **Industrial Systems (industrial IoT)**
- SCSs are systems whose **failure or malfunction can result in harm, injury or death, loss or damage to property, or impact to the environment**
- SCSs 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**

Objective 1: Specify a **Methodological Framework for the Design and Operation of Secure and Safe IoT Applications** addressing System Safety as a cross cutting concern.

Objective 2: Develop an **Open Cognitive IoT Architecture and Platform** (CHARIOT Platform), **intelligent safety behaviour** in the diverse and complex ways in which the safety critical system and the IoT system will interact in a secure manner

Objective 3: Develop a **runtime IoT Privacy, Security and Safety Supervision Engine** (IPSE)

- Privacy Engine based on PKI and Blockchain technologies
- Firmware Security integrity checking
- IoT Safety Supervision Engine (ISSE)
- Analytics Prediction and Dashboard

Objective 4: **Test and validate Industrial IoT safety in three Living Labs** (LLs) addressing different industrial areas in IoT safety

- Trenitalia (Italy)
- IBM Ireland Campus (Ireland)
- Athens International Airport (Greece)

Objective 5: **Scale up** through wide dissemination, exploitation, capacity building activities

IoT Devices' Lifecycle management

- Blockchain-based PKI for sensor and gateway authentication
 - Embedded keys in sensors and gateway (sensor controller)
 - Blockchain enabled gateway and server
 - CHARIOT sensors' prototype developments (Wifi and BLE)
- 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

- Eavesdropping /Interception/ Hijacking
- Man-in-the-middle attack
- IoT protocol high jacking
- Network reconnaissance
- Ruggedized communication protocol and encrypted communications between devices and controllers/gateways supported by blockchain
- Provisioning of all sensors in an IoT network through blockchain registration/affirmation
- Blockchain-based PKI for sensor and gateway authentication
- Four-eye-principle based sensor provisioning in the IoT network
- Dashboard-based solutions for sensor configuration, management and alerting

- Nefarious activities and Abuse
 - Malware
 - Denial of service
 - Software/hardware/ info manipulation
 - Targeted attacks
 - Abuse of personal data
 - Brute force
- Firmware static analysis avoiding software vulnerabilities (etc.) at source code and existence of backdoors, software scope alteration etc.
- Firmware binary checking against injected code at execution level avoiding Ransomware, viruses, Trojan horses and spyware
- Firmware hashing and meta data storage inside the binary (and blockchain) for increased software update assertion
- Orchestrating mechanism for sensor data ingestion, management, storage, normalization and external connectivity API
- Registration of sensor status and alerts in blockchain affirming transactions and events
- Private data automated flagging and reporting
- Safety engine managing topology, sensors deployment, commissioning and provisioning
- Data encryption policies based on blockchain technologies to avoid privacy breaches in the IoT network
- Dashboard-based solutions for sensor configuration, management and alerting

- Unintentional (accidental) Damages
- Unintentional configuration changes
- Damages by third parties
- Erroneous usage by administration
- Orchestrating mechanism for sensor data ingestion, management, storage, normalization and external connectivity API
- Machine learning anomaly detection based on user-defined models and neural networks
- loTL (language) for dynamic network configuration, access control rules and network topology definition
- Dashboard-based solutions for sensor configuration, management and alerting

- Failures and Malfunctions
 - Failure of sensor or device
 - Software vulnerabilities exploitation
 - Failure/malfunction of control system
 - Machine learning anomaly detection based on user-defined models and neural networks
 - Predictive analytics to highlight out-of-bounds behaviors and assess combined interdependent risks
- Legal
 - Contractual requirements
 - Violation of rules
 - Machine learning anomaly detection based on user-defined models and neural networks
 - Predictive analytics to highlight out-of-bounds behaviors and assess combined interdependent risks
- Physical Attacks
 - Sabotage / Vandalism
 - Out of CHARIOT scope for CHARIOT however support for malfunctioning devices is provided

SMART BUILDINGS (IBM campus)



Monitoring IoT devices and communication in a building (& rooms) environment, Enable IoT evolution to a cognitive IoT environment and Provide a safer & efficiently managed working environment.

- Utilization of sensor data during a fire hazard event
- Checks for security problems in the binary firmware updates on the CHARIOT fog server
- Uses Blockchain to encrypt the readings of presence sensors.
- Sensitive data privacy

RAIL (Trenitalia)



Monitoring the data traffic between the on-board IoT sensors (installed in the mechanic and electronic equipment of the train) and the Dynamic Maintenance Management System (DMMS).

- Early detection of anomalous data communication (distorted data)
- Early detection of unauthorized IoT devices (Gateway blockchain and SE checks on sensors' firmware)
- Early alerting for potential security violation (notify the security manager)

Airport (Athens International Airport)



Monitoring IoT devices and communication in an airport environment, fire alarm situations and intermediate security & safety layer, detect unusual patterns of signals from IoT devices.

- Enhance facilities protection on physical & cyber threats
- Early detection & prediction of hazardous situations
- Reducing the false positive alarms
- Warrantee the comfort and safety of the people located to the airport (travellers and employees).

- Technical Developments
- Technical Integration and Deployment
- Validation at Industrial Sites
 - Platform testing
 - New sensors developed
 - Interfaces and local connectivity
 - Functional and Operational performance
 - Dashboard and UI validation and feedback





Konstantinos Loupos, MBA, PMP, MSc, Meng
Head of R&D program, INLECOM
(CHARIOT project coordinator)
konstantinos.loupos@inlecomsystems.com



This project has received funding from the European Union's Horizon 2020 research and innovation program (No 780075). The authors acknowledge the research outcomes of this publication belonging to the CHARIOT consortium.