Integrated Solution for Industrial IoT Data Security – The CHARIOT Solution

Konstantinos Loupos, Alexandros Papageorgiou, Thomas Krousarlis, Antonis Mygiakis
Inlecom Innovation,
Athens, Greece
{name.surname}@inlecomsystems.com

Sofiane Zemouri, Magdalena Kacmajor
IBM Ireland Ltd,
Ballsbridge, Ireland
sofiane.zemouri1@ibm.com,
magdalena.kacmajor@ie.ibm.com

Harris Avgoustidis, Vassileios Kalompatsos
TELCOSERV,
Agios Stefanos, Greece
{h.avg, vkal}@telcoserv.gr

Christos Skoufis, Stelios Christofi, Vasos Hadjioannou
EBOS Technologies Ltd,
Nicosia, Cyprus
{christoss, stelios, vasosh}@ebos.com.cy

Andrea Battaglia, Andrea Chiappetta, Jacopo Cavallo
ASPISEC Srl,
Rome, Italy
{a.battaglia, a.chiappetta,
j.cavallo}@aspisec.com

Basile Starynkevitch, Franck Vedrine
CEA, LIST,
Gif-sur-Yvette, France
{name.surname}@cea.fr

Konstantinos Zavitsas
VLTN GCV,
Antwerpen, Belgium
kzavitsas@gmail.com

George Theofilis
CLMS Hellas,
Athens, Greece
g.theofilis@clmsuk.com

***Abstract*— The CHARIOT H2020 (IoT) project (Cognitive Heterogeneous Architecture for Industrial IoT), integrates a state-of-the-art inclusive solution for the security, safety and privacy assurance of data in industrial networks. The solution is based on an integrated approach for IoT devices lifecycle management (based on blockchain and public key infrastructure technologies), IoT firmware development and deployment (source and binary level vulnerability analyses), data analytics (privacy by design, sensitive data detection, dynamic network configurations etc.) and a set of user interfaces for management and control of the network, devices and the CHARIOT platform. CHARIOT is funded by the H2020 programme under the IoT topic, has a 3-year duration and concludes its activities by the end of 2020.**

Keywords*— *IoT, industrial data, security, privacy, safety

I. Introduction

The CHARIOT project is focusing its activities on an integrated solution towards recent risks and challenges of the industrial IoT domain. These include a wide span of cyber technological concerns and attacks that include: i) eavesdropping, interception and hijacking (man in the middle, protocol hijacking, network reconnaissance etc.), ii) Nefarious activities, abuse (malware, denial of service, software manipulation, targeted attacks, personal data abuse and brute force attacks), iii) unintentional damages (configuration changes, third party damages, erroneous usage etc.), iv) network failures and malfunctions (failure of sensor/device, software vulnerabilities, failure/malfunction of control systems) and v) legal (contractual requirements, violation of rules). The paper contribution is summarized to IoT Devices' Lifecycle management, IoT Firmware Development and Deployment, Intelligent IoT Data Analytics and IPSE and Platform and User Interface as components of the CHARIOT solution.

II. Industrial IoT Security Orientation

A. Industrial Requirements Overview

The requirements related to the CHARIOT project offerings are strongly related to recent challenges in modern IoT networks and mostly target sensing and monitoring systems in various industrial themes including smart buildings, airports and trains. All investigated scenarios require data exchanges in a safe, secure and private approach resulting into overall needs of trusting the actual sensors and information they convey in a complex network, guaranteeing thus the network devices accuracy and non-intrusion. These challenges have driven the CHARIOT solutions in placing the actual network devices as the 'root of trust' in these IoT networks [1] [2] [3].

CHARIOT central revolution and innovation over the current state of the art is oriented in placing the actual devices of an IoT network as the root of trust through its cohesive approach towards Privacy, Security and Safety (PSS) of industrial IoT Systems. This is achieved through a combination of Public Key Infrastructure (PKI) technologies coupled with pre-programmed private keys deployed to IoT devices with corresponding private keys in Blockchain for affirming/approving valid transactions, a blockchain ledger affirming various levels of operational/functional changes in the network (devices authorization, provisioning, status changes etc. as an audit log), a supervision engine combining supervision, analytics and predictive modelling over IoT data and a firmware development, validation and update approach (based on online and offline code/binary analyses) securing end-to-end code development and execution on the devices.

CHARIOT provides a series of unique and innovative management features for Industrial IoT and connected devices including providing devices' software and firmware level security and sensor visibility through a dashboard for, configuration, software updates management etc. By automating key sensor management functions using blockchain, PKI and automated workflows, CHARIOT provides a solution to coping with the fast pace growth of emerging IoT technologies whose pace of evolution is faster pace than skilled staffing and available resources while at the same time places the IoT devices as the root of trust (central innovation point in CHARIOT). In other words, CHARIOT automates key sensor management functions to improve their cost effectiveness. In this direction, CHARIOT, addresses the whole lifecycle of IoT devices and networks supporting various verticals.

B. Building Management Requirements and Challenges

In building management view, CHARIOT has investigated the IBM Technology campus (partner in CHARIOT) including thousands of sensors and actuators of varying types, functionalities and levels of sophistications deployed across six main buildings. These endpoints constantly monitor and report back to different systems such as safety and workplace management systems. The endpoints range from state-of-the-art fire detection sensors down to inexpensive heat sensors placed in computer racks in internal lab rooms by operations staff. These systems perform monitoring and control functions in an isolated manner. Each system is an IoT silo that has visibility over a limited area and has actionability to perform a constrained set of functionalities only. In addition, these heterogeneous systems contain different user interfaces, which makes it difficult for administrators to get used to and use them to their full potential. This makes the enforcement of campus wide safety and security policies extremely difficult to realise. In fact, in the best of cases, these systems only allow for basic analysis of aggregated and historical data collected through some datapoints spread across multiple silos on the campus. Visualization and reporting of intrusions, out of boundary behaviour as well as end to end devices lifetime monitoring (software upgrades etc.) are of primal importance and need.

C. Airport Environment Requirements and Challenges

In airport situations, as analyzed from the Athens International Airport (partner in CHARIOT), the primal importance of the operators is focusing on evacuation cases, passengers' comfort and maintaining smooth conditions in both cases. For this, monitoring/sensing systems are spread in various places of the airport infrastructure and continuously monitor the infrastructure sensor measurement to ensure in bounds behaviour. However, tampering (software or hardware) of these devices remains practically impossible (or very difficult), airport operators remain seriously alert in keeping up with modern IoT cyber security solutions and standards to avoid this. For this, recent cyber security implementations ensuring the data safety, security and privacy are of outmost importance in view of trusting the sensor data itself.

D. Train/Rail Environment Requirements and Challenges

Cooperation with TRENITALIA (as also a partner in CHARIOT), has revealed a different dimension also related to data security and privacy that relates to data collection for safety and predictive maintenance operations as well as efficiency management. This is seen usually in train (wagon) scenarios where collected data are analysed in modern systems to perform continuous monitoring of traffic flows, prevention, early detection, diagnosis and mitigation of the data breaching effect controlling the IoT sensors data package that are delivered to Dynamic Maintenance Management Systems. In this case, train operators need a system that checks the IoT communications and collects status reports informing the operator of potential security violations detected.

III. Overall CHARIOT Technical Orientation

In view of detailed analyses of the above requirements, CHARIOT is developing an innovative Privacy, Security and Safety (PSS) platform for IoT Systems, that places devices and hardware at the root of trust, in turn contributing to high security and integrity of industrial IoT.

The solution consists of a CHARIOT platform that integrates the various components and services of the solution integrated into a cohesive and dynamic approach. The main components consisting the CHARIOT solution include three run-time engines: i) privacy engine ii) security engine and iii) safety engine, each responsible for different layer of IoT data management and security. Machine Learning (ML) technologies are running in both the safety and privacy engines to ensure that data are inside the predictive boundaries and follow normal (and acceptable) operational behaviors inside the networks.

The solution also integrates recent research results on software level guarantees, including source code analysis (development time) and binary code analysis (execution time). These are strongly interconnected (via metadata interchanges into the security engine) to provide an end-to-end IoT devices lifecycle management and security at the firmware level.

A strong component of the solution includes a blockchain layer combining Public Key Infrastructure (PKI) technologies to affirm firmware or devices modifications storing the related information in a Distributed Ledger approach. This is used for both the devices' network registration (and commissioning) and also for the firmware updates (guarantees of IoT device firmware) from source code development up to the firmware update at the device. Operational and management dashboards serve as the User Interface (UI) for the platform and system operators including IoT sensors/devices commissioning, network setup, management and control as well as zones' definition and topology considerations.

As described above, a reference architecture integrates all above modules and technologies into a modern IoT solution span inside the cloud and fog layer of services. A high-level system description is included in the diagram below:

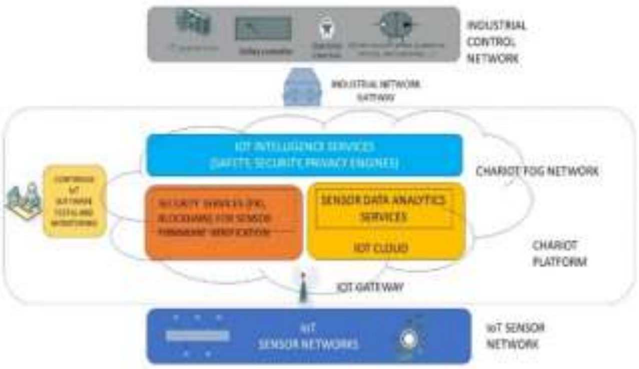

INDUSTRIAL CONTROL NETWORK
INDUSTRIAL NETWORK GATEWAY
IOT INTELLIGENCE SERVICES (SAFETY, SECURITY, PRIVACY ENGINES)
CHARIOT FOG NETWORK
SECURITY SERVICES (PKI, BLOCKCHAINS FOR SENSOR FIRMWARE VERIFICATION
SENSOR DATA ANALYTICS SERVICES
IOT CLOUD
CHARIOT PLATFORM
IOT GATEWAY
IoT SENSOR NETWORKS
IoT SENSOR NETWORK

Fig. 1. High Level CHARIOT System Design

More details for the operation and capabilities of the developed modules are described in the following sections in this publication.

The table below summarizes the technical orientation of CHARIOT over modern IoT threats and the particular components of CHARIOT

IoT Threat	CHARIOT Solution
▪ **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
▪ **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 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 IoT ▪ Dashboard-based solutions for sensor configuration, management and alerting
▪ **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 ▪ IoTL (language) for dynamic network configuration, access control rules and network topology definition ▪ Dashboard-based solutions for sensor configuration, management and alerting
▪ **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
▪ **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
▪ **Sabotage / Vandalism**	▪ Out of CHARIOT scope for CHARIOT however support for malfunctioning devices is provided

IV. The CHARIOT IoT Engines

CHARIOT integrates three (3) IoT data management layers responsible for performing operations on the data to verify and affirm their privacy, security and safety inside the IoT network. The components have been designed by taking into consideration the operation and scalability requirements of the three living labs participating in CHARIOT (rail, airport, smart buildings) into the IPSE (Integrated Privacy and Safety Engine). Safety here refers to Machine learning anomaly detection based on user-defined models and neural networks. The IPSE can be scaled out by distributing the runtime across multiple nodes if needed. A CHARIOT simulation tool will also be used internally to test the platform and overall system scalability and elasticity through exhaustive testing using large series of data that may not be available in the CHARIOT LLs but still pose a significant challenge in IIoT systems and networks. These are described below:

A. *Privacy Engine*

The CHARIOT Privacy Engine employs and integrates modern security protocols and technologies (e.g. Blockchain) to provide the foundation layer for the trusted interchange of information between the different network actors (sensors, nodes, devices, gateways, controllers etc.). The Privacy engine utilizes the IoT topology described with the IoTL language to ensure that only data from well-known sensors are accepted into the system. The IoTL language itself was extended with new concepts that can fully describe access control rules and allow access to sensor data only to specific systems, users, roles, etc. These new concepts also add semantics relevant to privacy, such as explicitly flagging a sensor as a sensitive data sensor, that can later be used e.g. to obfuscate or anonymize some or all properties of the data [4]. When a system needs to receive sensor data it must register its public key with CHARIOT's Blockchain-based PKI. The Privacy engine uses the PKI to get the public keys of the system that is allowed to receive sensor data and uses it to encrypt the data before sending them. This way only the owner of the private key can decrypt and access the raw data [4].

This component considers recent privacy issues in IoT systems including data being collected by individual sensors that should enter the system if only the sensor is known and registered in the topology and also if the data is from a known sensor, data encryption must be applied using a public key stored in a blockchain PKI. This module uses advanced cryptography in achieving protection towards confidential information stored in network and secure transmission over one network to another network. Cryptography is applied on the sensor data, immediately after, sensor data are verified over their receival from a (topology) well known sensor. CHARIOT has designed the encryption PKI engine so it can support multiple encryption algorithms and has initially adopted the RSA Cryptography algorithm for the first version of the Engine. The integrated blockchain layer provides valuable security features such as certificate revocation, elimination of central points-of-failure and a reliable transaction record that are otherwise unattainable by traditional PKI systems. Additionally, blockchain is applied as a public append-only log, naturally provides the certificate transparency (CT) property proposed by Google [5].

The CHARIOT Privacy engine ensures data privacy through encrypting data at the source, specifically at the southbound dispatcher through a PKI supported by CHARIOT blockchain infrastructure. Using CHARIOT Blockchain solution for handling PKI provides secure encryption for the multiple data streams handled by CHARIOT. Alert flags are raised in every case of sensitive data transfer through the fog-node; thus, the Network Administrator is informed in order to report accordingly.

To build the Privacy Engine, open source solutions and Python scripts have been used to develop this application. For encryption an RSA algorithm was used to complete the engine. The solution was packed as a docker container and it is available at GitLab Private Registry.

B. *Security Engine*

The CHARIOT security engine is responsible for the integrity and trust of the devices (sensors, gateways, controllers etc.) of the IoT network. This protects the devices (and network) against modern IoT attacks such as: i) reverse-engineer of the entire firmware (extract the file system and understand how the entire device works, knowing the possible use of known-to-be-vulnerable out-of-date API/libraries or unknown exploitable vulnerabilities), ii) insert a firmware backdoor (making the device covertly connected to a malicious Command & Control server), iii) change the device behaviour (altering its performance), iv) find hard-coded private symmetric-cryptography keys/passwords/user-names or private certificates (used to encrypt communications between the device and other systems and eavesdrop these communications) and v) roll-back the firmware to a previous legitimate version with known vulnerabilities he/she wants to exploit (verify if the pushed firmware is authentic, so it can easily survive most of the in-place controls, as usually, they tend to check just the firmware source and/or the firmware integrity) [6].

The CHARIOT security engine verifies the reliability of new issued firmware(s) during the tricky and demanding update phase using features detection and heuristic approach. The firmware verification analyses the firmware's binary that will be flashed on the end-device (sensor or gateway). The firmware analysis is performed during the firmware update process, and its purpose is to highlight any vulnerabilities inside the firmware code that could potentially lead to cyber-attacks. A created hash (during the firmware development stage) of the firmware is stored in the blockchain after the validation of the Security Engine. The hashing of the binary file is performed by the CHARIOT platform along with the keypair and the registration of the hashing to the blockchain. When a potential security issue has been found inside the reversed binary code of the firmware, the Engine reports a security violation to the management for the subsequent actions and analysis.

The heuristic method treats the system as different sub-systems so that the sub-system's solution must spread widely at the solution space. This approach is more appropriate since we have to deal with types of firmwares that are often very different from each other (in architectures/CPUs/ characteristics). Heuristic method brings several benefits, giving us flexibility in analysis, in fact we can combine different features as well as news instructions and features could be added as new functions with new parameters for analysis. This allows an analysis addressed by considering different aspects of the characteristics of the firmware, the change of its behavior and possible vulnerabilities that could be exploited to tamper the firmware, leading to a more complete and reliable analysis.

The utility is designed to collect data by binaries, perform statistical analysis, compare two firmware images and checking for vulnerabilities and formal contracts. The analysis is performed on the assembler instructions level. Based on the analysis results, a report is generated which contains information on the differences between the two images and if a vulnerability has been detected. An advanced attack pattern recognition helps to detect unusual hardware behavior and compares anomalies with an internal set of instruction that can lead to recognize an unknow attacks and exploitations [6].

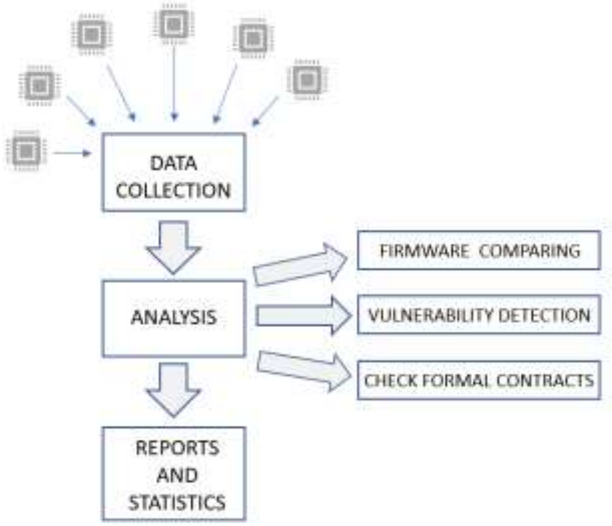


Fig. 2. CHARIOT Security Engine Model Implementation [6]

The CHARIOT security engine vulnerability detection layer provides the following vulnerability classes check: i) buffer overflow, ii) format string and iii) artbitrary memory access and reports its findings during the firmware update process to the platform and in-turn to the User Interface, accepting or declining/stopping the firmware update process.

C. Safety Engine

The CHARIOT Safety Engine analyses the IoT topology and signal metadata relative to the relevant safety profiles and applies closed-loop machine-learning techniques to detect safety violations and alert conditions. This comprises a later capability on the cognitive engine that will leverage the Cyber-Physical topological representation of the system-of-systems combined with the security and safety polices.

Anomaly detection aids finding patterns in data that do not conform to expected behavior [7]. Under IoT terms, anomalies are considered as any abnormal data stream pattern whose root cause may have safety security implications. These may be a faulty sensor, a safety hazard or a security issue. By identifying these issues and providing a central alerting mechanism, CHARIOT will help operators in reducing response time and identify root causes in cases of issues.

The CHARIOT security engine uses rule-based policies with simple arithmetic comparisons to enforce policies on data streams. An innovative IoTL (IoT scripting language -IOT Language) supports alerting the industrial gateway if a safety policy violation is observed within the IoT State. Furthermore, the security engine is using machine learning based anomaly detection.

In addition to a low-level Swagger API, IBM has developed a high-level UI for interfacing with the IoTL to facilitate interactions with the service topology as well as static and dynamic policies enforcement. The IoT Manager UI is implemented using the React and Leaflet libraries and features a Quake-style terminal for inputting IoTL commands [8].

V. Predictive Machine Learning Modelling

IoT data are in general characterized by volume, velocity and variety-lack of structure/heterogeneity. The frequent lack of structure in IoT data makes it difficult to analyze such data with traditional analytics and business intelligence tools. Additionally, IoT data that capture physical processes such as temperature, motion, or sound can be noisy. Finally, the quality of IoT data can vary, i.e. datasets can have significant gaps, and contain corrupted readings. Lastly, meta-data/context may be essential to understand IoT data, as such data are often meaningful in some context. IoT data typically contain patterns that include seasonal fluctuations and trends. Such patterns must be detected amongst noise, random fluctuations and other non-important findings. IoT analytics systems can filter, transform, and enrich the IoT data before storing it, usually in a time-series data store for analysis. Insights from the IoT analytics are then used to better understand the system measured by the IoT sensors and to make better decisions.

Anomaly detection refers to the problem of finding patterns in IoT data that do not conform to some norm [9]. These non-conforming patterns are often referred to as anomalies, (and also as outliers, exceptions, aberrations, etc.) in different contexts. Anomaly detection has wide applicability in a variety of IoT applications such as for security protection and fault detection in industrial systems. One major application of anomaly detection, of relevant to CHARIOT is fault detection in mechanical units. The anomaly detection techniques in this domain use IoT to monitor the performance of industrial components such as motors, turbines, and other mechanical components to detect when maintenance of the system will be required (‘predictive maintenance’).

CHARIOT is using several different methodologies for the anomaly detection layer including: i) One Class Support Vector Machine (OSVM) - trained using both positive and negative examples, however studies have shown there are many valid reasons for using only positive examples, ii) Elliptical Envelope (EE) - based on the Minimum Covariance Determinant (MCD) estimator the first affine equivariant and highly robust estimators of multivariate location and scatter and iii) Isolation Forest (IF) - efficient unsupported machine learning algorithm for anomaly detection focusing on identifying the few different points of the dataset, rather than the normal data, and uses the isolation mechanism that detects anomalies purely based on the concept of isolation without employing and distance or density measure, which is fundamentally different from previously described methods [11].

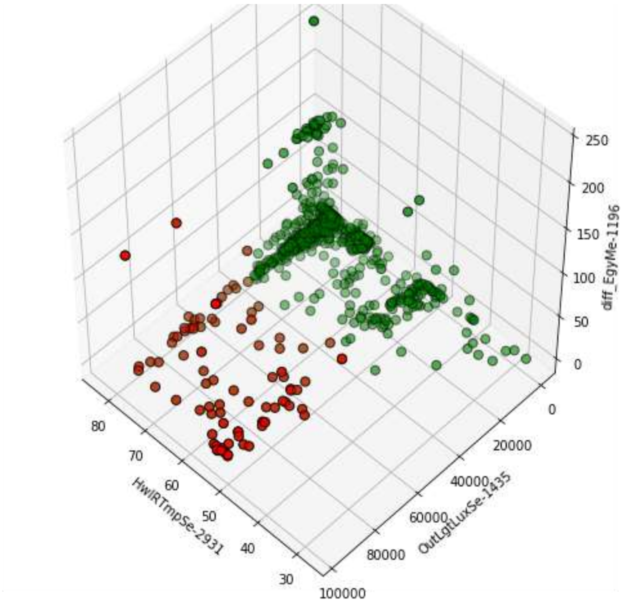


Fig. 3. Example of Anomaly Detection Modelling

VI. Software Life-Cycle Management

The CHARIOT software analysis and lifecycle management includes a software source code verification analysis level (Bismon) that is strongly linked to the CHARIOT security engine (and the firmware update process). This, includes the source code analysis, creation of metadata and hashing of source code inside the binary file that are analysed during the firmware update process (via the security engine and together with the binary level warnings) to either accept or decline the software update process.

CHARIOT focuses mainly on a system of systems (e.g. networks of systems and systems of networks) approach, so [10] "aims to address how safety-critical-systems should be securely and appropriately managed and integrated with a fog network made up of heterogeneous IoT devices and gateways.". Within CHARIOT, static analysis methods support its Open IoT Cloud Platform through its IoT Privacy, Security and Safety Supervision Engine. Some industrial CHARIOT partners, while being IoT network and hardware experts, acknowledge that their favourite IDE (provided by their main IoT hardware vendor) is running some GCC under the hoods during the build of their firmware. Nevertheless, these partners do not use static source code analysis tools.

The CHARIOT approach to static source analysis leverages on an existing recent GCC cross-compiler [11] so focuses on GCC-compiled languages [12]. Hence, the IoT software developer following the CHARIOT methodology would just add some additional flags to existing gcc or g++ cross-compilation commands, and needs simply to change slightly his/her build automation scripts (e.g. add a few lines to his Makefile). Such a gentle approach (see figure 1) has the advantage of not disturbing much the usual developer workflow and habit, and addresses also the junior IoT software developer. The compilation and linking processes are communicating -via some additional GCC plugins (cf. GCC Community [6] §24) doing inter-process communication- with our persistent monitor, tentatively called bismon. It is preferable (see Free Software Foundation) to use free software GCC plugins (or free software generators for them) when compiling proprietary firmware with the help of these plugins; otherwise, there might be some licensing issues on the obtained proprietary binary firmware blob, if it was compiled with the help of some hypothetical proprietary GCC plugin.

CHARIOT static analysis tools will leverage on the mainstream GCC compiler (generally used as a cross-compiler for IoT firmware development). Current versions of GCC are capable of quite surprising optimizations (internally based upon some sophisticated static analysis techniques and advanced heuristics). But to provide such clever optimizations, the GCC compiler has to be quite a large software, of more than 5.28 million lines of source code (in gcc-8.2.0, measured by sloccount). This figure is an under-estimation, since GCC contains a dozen of domain specific languages and their transpilers to generated C++ code, which are not well recognized or measured by sloccount.

Since a single Bismon process is used by a small team of IoT developers, it provides some web interface: each IoT developer will interact with the persistent monitor through his/her web browser. In addition, a static analysis expert (which could perhaps be the very senior IoT developer of the team) will configure the static analysis (also through a web interface) [13].

VII. Supporting Blockchain and PKI Technologies

The blockchain component of CHARIOT (based on a hyperledger Fabric implementation) is used at different engines and layers to affirm data, devices and network information. In this, the information stored in blockchain include sensor IDs, network states and firmware validation hashings. These are used by the privacy, security and safety engine as described before.

Blockchain-based PKI approach makes MITM attacks virtually impossible as when group of authorities publishes or revokes the public key of an identity on the blockchain, the information will be distributed across all nodes, so tampering the public-key will be (theoretically) out of the question. Traditional PKI resolves MITM risks by embedding Root CA certificates into browser installations, thus artificially expanding CA entrance barriers and increasing the time necessary for Root CA certificate revocation.

There are several advantages of using this PKI-based blockchain implementation including: i) The validation of a certificate is simple and fast with no form of CA certificate chain, ii) Blockchain-based PKI solves a longstanding problem of traditional PKIs by not requiring the use of a service that issues certificate revocation lists (CRLs) thanks to blockchain synchronization between network's nodes where any modification to the state of a certificate will be instantaneously notified to the all nodes and iii) Blockchain-based PKI provides flexible protection against the man-in-the-middle (MITM) attacks. Traditionally, MITM is considered as a major security risk implying attacker to hijack a browser's connection for a given website by presenting a valid certificate (i.e., forged public key) for that domain. For users and web browsers it is difficult to identify the replacement of certificate when the related CA has been hacked by the attacker [7] [8].

VIII. Operational and Device Management Dashboards

User interfacing is considered as an important layer where two distinct interfaces (dashboards) are being developed (Device Management Dashboard: handling blockchain devices registration, firmware updates, engine management and IoTL interfacing and Operational Dashboard: providing Engines' health and performance monitoring as well as alerts' and sensor data visualization).

The device management dashboard is utilizing the latest state-of-the-art web technologies to deliver rich content information to the LL users and achieve cross-browser and multi-device compatibility. Further to that, the dashboard is designed as a user friendly and fully responsive web solution, based on the CHARIOT industrial needs, providing an easy access to the necessary information. Blockchain security and accessing controls are applied to secure the access to specific information and data by different users. Moreover, Dashboards focus not only to standard monitoring actions and providing a visibility on an industrial IoT topology, sensor values and alerts but also to secured (utilizing blockchain technology) managerial activities. Those activities such as authenticating and registering (or unregistering) a sensor in the IoT topology and updating the firmware (of a sensor or a gateway) can be performed by the security engineers and management. It is important to mentioned that during the "firmware update" there is a chain of actions and integration with a number of CHARIOT components.

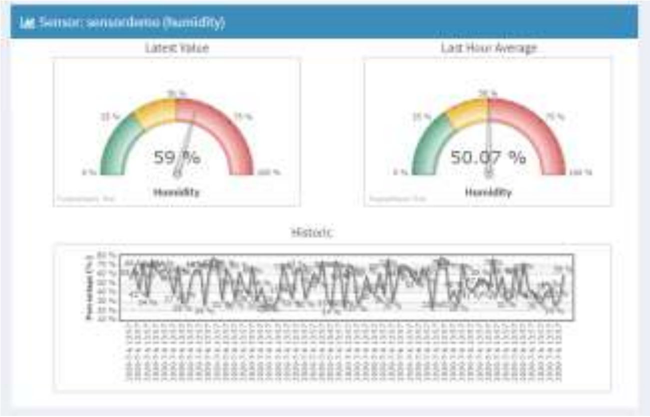
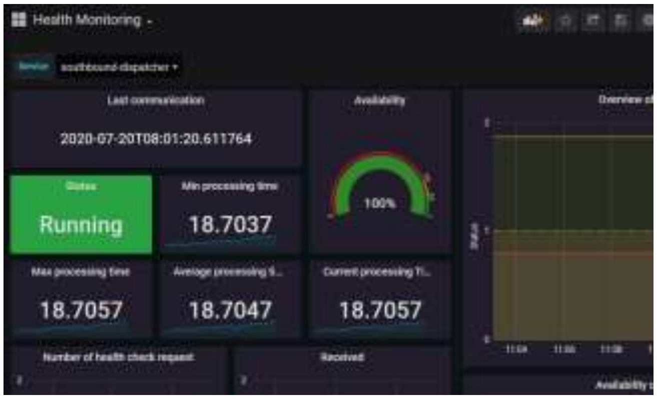


Fig. 4. Example of Data Management Dashboard

The CHARIOT Operational Dashboard is providing Engines' health and performance monitoring as well as alerts' and sensor data visualization. CHARIOT has identified the need of a more sophisticated method for platform performance monitoring as designed following the micro-services software architecture paradigm. After research on the industry-standard of micro-service platform monitoring techniques, CHARIOT has decided to adopt CNCF best practices and deploy Jaeger. With Jaeger, we can trace every action trail at the CHARIOT platform. The analysis of the collected traces helps the developer to identify bottlenecks to improve system performance and find the cause of platform malfunction. In addition to this, we implement service to monitor health of every micro-services by sending a "magic-package" to it and then wait for its response, in the end the system administrator has a dashboard to view all the collected information [14].



Last communication: 2020-07-20T08:01:20.611764

Availability: 100%

Status: Running

Min processing time: 18.7037

Max processing time: 18.7057

Average processing ti...: 18.7047

Current processing Ti...: 18.7057

Fig. 5. Example of Operational Dashboard

IX. CHARIOT Industrial Validation

CHARIOT is by design driven by industrial IoT requirements following actual needs and paradigms of three sectors: rail, airports and smart buildings. These three industrial cases' analysis has derived exhaustive sets of requirements, industrial scenarios and validation KPIs on which, CHARIOT, has based its technical implementations.

CHARIOT will be validated in the above three (3) industrial cases based on representative security related scenarios highlighting the value and integrated approach of CHARIOT in solving modern IoT security issues and challenges.

CHARIOT is currently through its deployment and validation phase, having deployed its whole platform in the three infrastructures and having performed its first round of technical recommendations from the end-users. In the next five months, and up to the end of 2020, CHARIOT is expected to finish its activities with the final feedback of recommendations and adaptations to the three industrial setups.

Acknowledgments

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.

References

[1] K. Loupos - INTEGRATED SOLUTION FOR PRIVACY AND SECURITY OF IOT DEVICES IN CRITICAL INFRASTRUCTURES, Critical Infrastructure Protection and Resilience Europe (CIPRE 2020), 6-8 October 2020, Bucharest, Romania.

[2] K. Loupos, A. Papageorgiou, A. Mygiakis, B. Caglayan, B. Karakostas, T. Krousarlis, F. Vedrine, C. Skoufis, S. Christofi, G. Theofilis, H. Avgoustidis, G. Boulougouris, A. Battaglia, M. Villiani - COGNITIVE PLATFORM FOR INDUSTRIAL IOT SYSTEM SECURITY, SAFETY AND PRIVACY, Embedded World 2020 Conference and Exhibition, 25 - 27 February 2020, Nuremberg, Germany.

[3] Adel S. Elmaghraby, Michael M. Losavio, "Cyber security challenges in Smart Cities: Safety, security and privacy", Journal of Advanced Research Volume 5, Issue 4, pp 491–497, 07/ 2014.

[4] CHARIOT – D3.2 – IoT Privacy Engine based on PKI and Blockchain technologies, CHARIOT 2019.

[5] L. Axon and M. Goldsmith, “PB-PKI: A privacy-aware blockchain based PKI,” in Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4: SECRYPT, Madrid, Spain, July 24-26, 2017., 2017, pp. 311–318.

[6] CHARIOT - D3.8 – IoT Security Engine based on vulnerability checks, CHARIOT 2020.

[7] Chandola, Varun, Arindam Banerjee, and Vipin Kumar. "Anomaly detection: A survey." ACM computing surveys (CSUR) 41.3 (2009): 15.

[8] CHARIOT – D3.9 - IoT Safety Supervision Engine (ISSE) (final prototype) v1.0_FINAL, CHARIOT, 2020.

[9] Chandola, Varun, Arindam Banerjee, Vipin Kumar. Anomaly detection: a survey. ACM Computing Surveys, September 2009.

[10] Taken in October 2018 from https://www.chariotproject.eu/About, §Technical Approach.

[11] The actual version and the concrete configuation of GCC are important; we want to stick -when reasonably possible- to the latest GCC releases, e.g. to GCC 8 in autumn 2018. In the usual case, that GCC is a cross-compiler. In the rare case where the IoT system runs on an x86-64 device under Linux, that GCC is not a cross-, but a straight compiler.

[12] The 2019 Gnu Compiler Collection is able to compile code written in C, C++, Objective-C, Fortran, Ada, Go, and/or D.

[13] CHARIOT – D1.5 - Specialized Static Analysis tools for more secure and safer IoT software development (ver.2).

[14] CHARIOT – D6.9 – CHARIOT Rescoping Guideline