Automation for Industry 4.0 by Using Secure LoRaWAN Edge Gateway, based on STM32 MP1 DK2 System-on-Chip

June 2, 2021

The Hellenic Mediterranean University, Intelligent Systems & Computer Architecture (ISCA) Laboratory, in cooperation with ST Microelectronics, Grenoble, FR, has designed a Secure LoRa Gateway based on STM32 MP1 microprocessor. Developed within the framework of the Horizon 2020 Avangard project, this prototype enables the remote monitoring of industrial facilities and/or electric vehicle micro-factories while ensuring high security.

The AVANGARD project integrates three novel processing units into an existing micro-factory test bed conceived to produce urban electric vehicles. The pilot will be demonstrated manufacturing electric bikes and cars and innovative battery packs. One of the objectives is to achieve an agile production system implementing a reliable and secure communication infrastructure (industrial middleware) to support the vertical integration plug-and-produce production resources with higher level applications.

The introduction of low-power wide-area networks (LPWAN) with technologies such as LoRa has made it possible to build a low-cost communication infrastructure based on the LoRaWAN connectivity protocol that enables low-power and long-range transmissions of IoT devices via LoRaWAN gateways. These gateways act as a bridge between the IoT devices and the Cloud management layer: receiving the digitized data from sensors and routing it to the Internet for further processing.

The innovative LoRaWAN gateway (STM32MP157f-DK2 with a LoRa Concentrator module based on Semtech SX1301) is equipped with ARM Trustzone, STM security extensions, and adds an extra layer of security to the existing LoRaWAN infrastructure via the secure (verified) boot and the Trusted Execution Environment (TEE). In an ecosystem dominated by IoT with applications and data migrating to the cloud, and an increasingly sophisticated attack landscape in unsafe network environments, the STM32MP1x-based platform enables a security mindset for industrial networked environments. As attacks become more sophisticated, involving identity forging, hacking, phishing, key logging, denial-of-service (DoS) attacks, it is imperative to design robust devices and gateways that are impenetrable to any attempt to compromise the security of IoT devices and services.

The STM32 MPU is based on the Arm® Cortex®-A core, which uses Arm TrustZone architecture to enable execution context isolation: the normal world contains the applications whereas the secure world isolates all the trusted applications and core secure services so that they can safely manipulate platform secret data. The MPU includes firewall mechanisms that allow the secure world to forbid read/write access from the normal world to given peripherals.

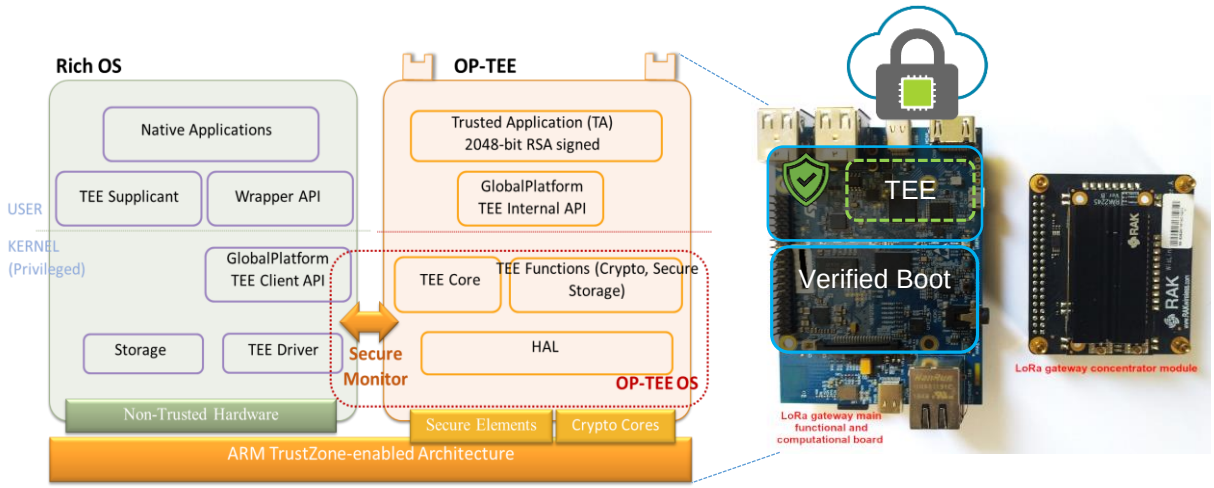

Figure 1. Secure LoRaWAN gateway through supporting trusted boot-chain and OP-TEE

When an STM32MP1 DK2 platform is used in a LoRaWAN infrastructure the MPU guarantees secure, trusted boot-chain, a Trusted Execution Environment (TEE) by using OP-TEE framework, and crypto, key management, storage, and certificate management via trusted applications. In addition, it provides a flexible Backhaul connection wired via ethernet or cellular using optional 3G / LTE modem such as Quectel BG96 worldwide cellular modem LTE Cat M1/Cat NB1/EGPRS module.

In summary, the supported features enabling Device-to-Gateway and Gateway-to-Cloud trusted computing and communications include:

- Secure Boot-chain
- Cryptographic, Key Management Storage, OpenSSL API
- Cryptographic, Storage and Certificate Management Trusted Firmware
- Firmware access control
- Firmware encryption
- Secure data storage
- Secure over-the-air firmware updates.
- 10 parallel demodulation paths, supports 8 uplink / 1 downlink channels.
- Ethernet or 3G / LTE Backhaul Network

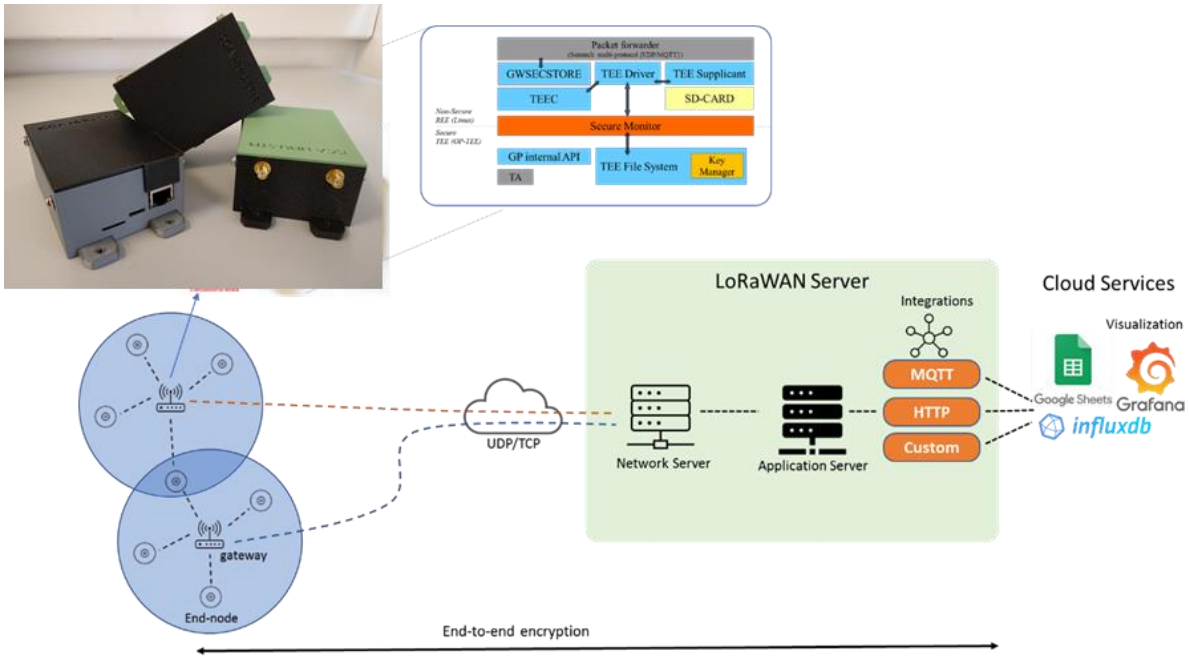

Figure 2. LoRaWAN architecture for Industrial IoT environment

Using different software packages developed by ST and with the support of microcontrollers division, the LoRaWAN edge gateway based on STM32MP1 has been fully integrated into an overall industrial monitoring system. The system is designed to seamlessly connect to the LoRaWAN cloud platform provided by The Things Network and state-of-the-art technologies for leading time-series DB (such as InfluxDB) and dashboards (such as Grafana) as shown in the illustration (see Figure 2).

Othon Tomoutzoglou *is a system architect and developer at the Hellenic Mediterranean University, Intelligent Systems & Computer Architecture (ISCA) Group. He has a master's degree in Informatics and Multimedia from the Technological Educational Institute of Crete. His interests include hardware design, embedded, reconfigurable and cyber-physical systems, and network security.*

Dimitris Mbakoyiannis *is a system engineer at the Hellenic Mediterranean University, Intelligent Systems & Computer Architecture (ISCA) Group. He has a B.Sc. degree from the Technological Educational Institute of Crete. His interests include embedded, reconfigurable systems, network security and cyber-physical systems.*

George Kornaros *is an Associate Professor at the Electrical and Computer Engineering Department, Hellenic Mediterranean University, Greece, where he leads the Intelligent Systems & Computer Architecture (ISCA) Group. His research interests include multi-/many-core systems, security, high-speed communication architectures and energy-efficient and heterogeneous computing. Kornaros has published more than 70 scientific articles, and edited the book "MultiCore Embedded Systems". He holds three patents and is a member of the Technical Chamber of Greece.*