RESEARCH-ARTICLE

A Secure LoRaWan Architecture and Infrastructure Approach

JOEL D GUERREIRO, University of Algarve, Faro, Faro, Portugal

Open Access Support provided by:

University of Algarve

Published: 31 July 2025

DSAI 2024: 11th International Conference on Software Development and Technologies for Enhancing Accessibility and Fighting Info-exclusion
November 13 - 15, 2024
Abu Dhabi, United Arab Emirates

DSAI '24: Proceedings of the 11th International Conference on Software Development and Technologies for Enhancing Accessibility and Fighting Info-exclusion (November 2024)
https://doi.org/10.1145/3696593.3696631
ISBN: 9798400707292

A Secure LoRaWan Architecture and Infrastructure Approach

Joel D Guerreiro
Instituto Superior de Engenharia, Universidade do Algarve
PT
jdguerreiro@ualg.pt

Figure 1: Implemented LoRaWAN Network 2024

Abstract

The Internet of Things (IoT) has been widely implemented for objects, uniquely identified, to become accessible through the internet. Several communication protocol technologies were studied and applied to interconnect objects using the internet. Nowadays, one of the most used is Low Power Wide Area Network (LPWAN) implemented over Narrow Band-Internet of Things (NB-IoT) or Long Range Wide Area Network (LoRaWAN) platforms. In this paper, a LoRaWAN architecture and infrastructure implementation is addressed to secure data and communications protecting Network Servers and communication between gateways and the demilitarized zone (DMZ), using several secure techniques and infrastructure virtualization software for containers.

CCS Concepts

• **LoRaWAN Networks**;

Keywords

LoRa, LoRaWAN, Cryptography, AES, Architecture, Security

ACM Reference Format:
Joel D Guerreiro. 2024. A Secure LoRaWan Architecture and Infrastructure Approach. In *11th International Conference on Software Development and Technologies for Enhancing Accessibility and Fighting Info-exclusion (DSAI 2024), November 13–15, 2024, Abu Dhabi, United Arab Emirates.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3696593.3696631

DSAI 2024, November 13–15, 2024, Abu Dhabi, United Arab Emirates

ACM ISBN 979-8-4007-0729-2/24/11
https://doi.org/10.1145/3696593.3696631

1 Introduction

Municipalities are today using IoT to manage different kinds of data, like water management, waste management, energy consumption, mobility, tourism and others, creating intelligence from the gathered data, automating different aspects for a better daily life in the cities [9]. A network technology, LPWAN, has a wide range and needs to use little power to communicate, supporting technologies like NB-IoT, LoRaWAN and SigFox [35]. LoRaWAN is being used in several different systems, like agriculture, fish farms, photovoltaic grids and on smart cities monitoring [22], widely used because it provides low-cost and bi-directional communications with a spread spectrum technique on free-use frequency bands for the IoT [8] [9] and its easy to deploy. LoRaWAN also demonstrated security resilience and robustness [15], [6], making the technology, along side with 5G, essential for massive IoT environments [10].

The Portuguese Lagos Municipality main objective was to implement a wide full coverage LoRaWAN Network, addressing the needed communication between sensors (smart objects) and Network Server integrating data into each vertical to provide better services to the population, being able to implement sensors in all Municipality area.

In this article, a distinct LoRawAN Network architecture and infrastructure implementation is addressed, in order to secure the network, all communication and the gathered data from the smart objects.

The remainder of this article is organized as follows: in Section 2 the used technologies are described, in Section 3 Related Work is presented. The Secure LoRaWAN architecture and infrastructure is addressed in Section 4, secure communications are presented in Section 5, in Section 6 the Resilient and Security tests performed and Section 7 concludes the article.

2 Technologies Overview

IoT allows physical objects to be accessed and controlled using the internet where trillions of smart things can be able to communicate in different areas [12].

LPWAN, using an unlicensed spectra, extends IoT solutions and enables the market with a wide area constrained network connecting low-powered devices [14], allowing constraint sensors to communicate and generate data that can be used in any area.

LoRaWAN emerged to facilitate communications in wide area networks where gateways relay messages from physical objects into a central network server based on the LoRa Alliance Standard [3]. LoRaWAN has a type of LPWAN that permits low-speed long-distance communication [11], consuming small amount of power while transmitting [34], being therefore an advantage for the physical constrained small batteries objects. As previously mentioned, the LoRaWAN architecture communication is established between physical smart object nodes and a network server in a star topology [21] offering nodes and gateways remote control, being able to receive communications from thousands of nodes in a large area [20].

In Figure 2 the implementation of a standard LoRaWAN architecture is presented, where all physical smart objects communicate with the Gateways using the LoRAWAN wireless capacity, sending data from time-to-time depending on the implemented schedule,

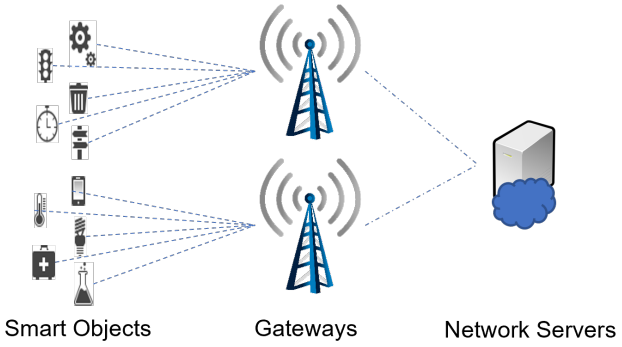

Figure 2: LoRaWAN Architecture

being redirected into the Network Server(s) for storage. The vertical applications read from the supported Application Programming Interface (API) available on the Network Server(s) into their databases so that the data may be monitored, organized and made available for users to manage the specific area.

As mentioned, LoRAWAN is optimized for low power consumption and designed to support millions of smart devices, so security must also be designed to consume low power, complexity, cost and high scalability [2]. With many distributed connected devices and massive communications brings to LoRaWAN networks, security risks, therefore is needed a resilient infrastructure and secure communications.

For a better understanding on how standard LoRaWAN security is implemented, Olivier Seller [29] explained that LoRaWAN security fundamental properties are authentication, integrity protection and confidentiality, relying on Advanced Encryption Standard (AES) cryptography algorithms combined with Cipher-based Message Authentication Code (CMAC) for integrity and Counter Mode Encryption (CTR) for encryption. Each LoRAWAN network device uses a unique 128 bit randomly generated AES root Key denominated AppKey, a global identifier EUI-64-Based DevEUI to identify the device roaming in the network and a Join Server identifier (EUI-64-Based JoinEUI) to identify what Join Server shares the secret AppKey with the device. All together are used for device activation. The author also states that all LoRaWAN Networks are identified by a 24-bit global unique identifier assigned by the LoRa Alliance, called NetID. Olivier Seller refers that LoRaWAN security has an end-to-end encryption for the exchanged payloads between end devices and Application Servers, where the Network Server authenticates and verifies the messages integrity transmitting the payload over a standard secured IP connection, so the Application Server is able to decipher the payload. All traffic is protected using two session keys, Appskey encrypts with 128-bit AES-CTR each payload and 128-bit NwkSKey network session key with 128-bit AES-CMAC encrypts each Message Integrity Code (MIC) that is used to avoid packet tampering. AES-CTR encryption generates distinct streams for uplink and downlink due to the direction being part of the input along with Devaddr, Frame counter (FCnt) and Key. The frame counter is incremented on each frame and cannot be reused with the same NwkSKey and AppSKey. Olivier Seller states that the Link control field is composed with frame type,

protocol version, acknowledgments, device operation mode, MAC commands and adaptive data rate signaling. This fields are not encrypted but are protected, authenticated and integrity checked. MAC commands can either be in the Link control field or sent as application data where the frame payload is composed by the MAC commands, and the AppKey is replaced with NwkSKey to encrypt the payload using AES-CTR encryption, making possible to transmit several MAC commands in on message. The AES-CTR mode decryption uses the same operation as the encryption, limiting, therefore, the complexity, implementing one operation for authentication and another for decryption. To activate the devices it can be used Activation By Personalization (ABP) or Over The Air Activation (OTAA), and the devices must be equipped with DevAddr, NwkSKey and AppSKey. When the activation starts, NwkSKey and AppSKey is stored on both device and Network Server with a prefix AddrPrefix to identify the network, enabling roaming for the gateways to redirect the traffic to the Network Server.

Another technology overview is Docker containers representing a lightweight, self-contained executable package with all essential components to execute a specific application [33]. Docker is an Operation System (OS) level virtualization that enables the creation of a isolated environments facilitating the development, deployment and application management throughout several systems, providing isolation and confining applications within sandboxes preventing any interference with the OS or other containers [25]. Despite being a secure and isolated environment, several concerns have been addressed with the microservices deploy using Docker containers [31]. Kun Suo et al [32] state that containers provide less security isolation than Virtual Machines (VMs). On the network isolation aspect there is a lack of effectiveness in the containers [23] and network attacks may occur if traffic is not efficiently separated [5].

In Section 3 the related work is presented where the all overviewed technologies were applied with several contributions made by the authors.

3 Related Work

Many approaches in implementing LoRaWAN networks have been addressed, with distinct objectives, but all with the same goal, to interconnect physical energy constrained devices with the network server to receive data in order to manage an area or vertical.

The authors Sokratis Katsoulis et al [19] implemented a LoRaWAN-based Vibration Detection Sensor network focusing on monitoring vibration initiation and ending, collection environmental data, transmitting the LoRa packets payload in a urban and rural fabric town, providing real-time notifications. The proposed infrastructure is based on a LoRaWAN basic architecture at the network edge using a Message Queue Telemetry Transport (MQTT) protocol connection to the Gateway, that receives and stores the data into a database. The vertical application server consumes the data from the database, and users are able to visualize the services using mobile applications. Extensive network coverage and end nodes communication were done successfully.

Sneha K. et al [18] developed an helmet to monitor hazardous activities like temperature, humidity and harmful gases concentration for the mining industry in order to ensure miners safety using LoRaWAN network technologies due to the wide range capacity. The system alerts the worker whenever any hazardous activity occurs vibrating the helmet, assuring workers safety.

An application of LoRAWAN in agribusiness was addressed by Alfredo Arnaud et al. [4] using a survey with over 1500 commercial sensors and cameras, with a single LoRaWAN Gateway, over a 1000ha cattle field to estimate efficiency. Results show over 92% efficiency in all cases with a small but not negligible error percentage in communication.

The performance on Edge-Cloud network server structure to LoRaWAN networks providing a standardized edge computing LoRaWAN infrastructure was presented by Zhify Zhang et Al. [36]. The developed work uses network queuing to analyze quantitatively the performance applied to LoRaWAN and IEEE 2668, consisting in a edge server, a cloud server and requesting service clients. The LoRaWAN network consists in end node devices, network server, Gateways and Application server. Results show that the model illustrates the evaluation parameters that can be used and propose a IEEE 2668 LoRaWAN edge computing infrastructure evaluation index.

An LoRaWAN and Wireless Local Area Network (WLAN) evaluation for monitoring IoT-based photovoltaic microgrid systems was presented by Muhammad 'Aamir Nashrullah et al [26] assessing the capability of wireless communications in gathering photovoltaic systems data in urban areas. Coverage, latency, Received Signal Strength Indication (RSSI) and Packet loss were the key parameters studied in a coverage area of 74102 square meters. Besides WLAN be able to have a higher data transfer rate and less latency, LoRaWAN excels in stability with 0.5% packet loss.

An Intelligent Urban Expressway Managing LoRaWAN and Edge Computing architecture was addressed by Mi Chen et al. [7] dividing the traffic in two different section, LoRaWAN network for monitoring and controlling, exploiting lower-power and long-range features and a Edge computing traffic encoder model to handle the generated amount of data produced by the node massive number. Results show that the presented LoRAWAN architecture demonstrate high performance and scalability and the encoder model reduced effectively the packet size by extracting data features.

A security vulnerabilities analysis in LoRaWAN Smart City was researched by Siti Yusoff et al. [16] to evaluate LoRaWAN protocol performance under jamming attacks (stopping data flow communication) in a smart city environment network, using NS-3 network simulation software to conduct attacks at physical and Medium Access Control (MAC) layer. The authors state that several studies indicate LoRaWAN networks are vulnerable to attacks at MAC and upper layers. Results show a massive impact on packet loss as the number of jammers increase.

Efficient key management for a resilient LoRaWAN-based Smart Grip operation Applications was presented by Yacoub Hanna et al. [13]. The authors propose a new protocol for group key management and renewal reducing the message number and minimizing the process total delay. Using Diffie-Hellman (DH) key exchange with the authors secret sharing protocol to generate the group key initiating random pairing point and applying Lagrange interpolation and the hash-chain concept to renew the group key using a single message, reduces not only the number of exchanged messages but also diminishes significantly the total setup delay.

Jorge Navarro-Ortiz et al. [27] proposed a cost-effective solution to provide hardware security into end-devices. The authors propose the implementation of 3GPP Security that generates an attach request, an authentication vector containing a random number, a token, the ciphering and integrity keys and the expected response. With this 3GPP the device and data are authenticated using USIM cards, and stated that end-devices will no longer be vulnerable to security threats such as impersonation or cloning attacks.

An Advanced AES-Based Cryptographic Approach was addressed by Samira Abboud et al [1] proposing a AES 256-bit key instead of 128-bit key as an encryption model for LoRaWAN networks. To evaluate, metrics like security level, network throughput and end-devices energy utilization were analyzed. Results show that the LoRaWAN resilience against cyber attacks increased substantially and only a marginal disparity regarding network throughput and energy consumption, being a better trade-off between the increased security compared with a addition on network and energy consumption performance.

Lorenzo Parri et al [28] implemented a real-time monitoring LoRaWAN infrastructure based on fixed nodes and mobile sinks to remotely control offshore sea farms for data transmission. The authors were able to communicate up to 8.33 km offshore distance maintaining network reliability, measuring water quality and their maintenance status. A hybrid prototype solution architecture infrastructure was used where the sensor nodes transmitted encrypted LoRa packets and the remote server used MQTT protocol. The LoRa packets payload were encrypted twice using Network Session Key (NwkSKey) and Application Session Key (AppSKey) over Advanced Encryption Standard (AES). After encryption is done, the LoRa packets are then broadcasted to any listening Gateway to be, afterwards redirected using a MQTT client to the Network Server. The Network Server receives the MQTT packets in a inside MQTT broker, storing the data into the database.

Securing MQTT communications framework in a food retail distribution was proposed by Mattia Spina et al [30] considering several attacks like Man-in-the-Middle, Dictionary, Data forgery and SlowIte to target the communication among the smart devices, proposing a mitigation methodology for each of them. The architecture proposed uses a MQTT Broker that manages the product information and the communication. A shelf sensor was used to measure the amount of products in a shelf. Results show that the proposed framework achieves better results compared with the standard MQTT with TLS system.

Drake Mubanda et al [25] used penetration testing methodologies to study Docker Containers vulnerabilities uncovering misconfigurations and potential intrusion vectors by exploring the file system and artifacts that can be exploited. The results show that the discoveries empower system administrators to enhance container defense strategies and proactive diminish security risks.

A design to attain a required level of network isolation in Docker Containers was presented by Asem Mousa et al [24] using a firewall container acting as a gateway connected to a virtual bridge in order to protect the containers from unauthorized accesses and Man-in-the-Middle attacks. The firewall was configured to filter traffic and port forwarding using Network Address Translation (NAT) and a Dynamic Host Configuration Protocol (DHCP) server. The proposed design provides extra isolation and separates the container network stack from the Docker containers, hardening the system with a virtual switch between the service containers and the firewall that controls the hidden services using IPTABLES rules. Results were successful and the design was able to isolate network internal network containers from the host, other containers and the outside mitigating therefore network-based attacks.

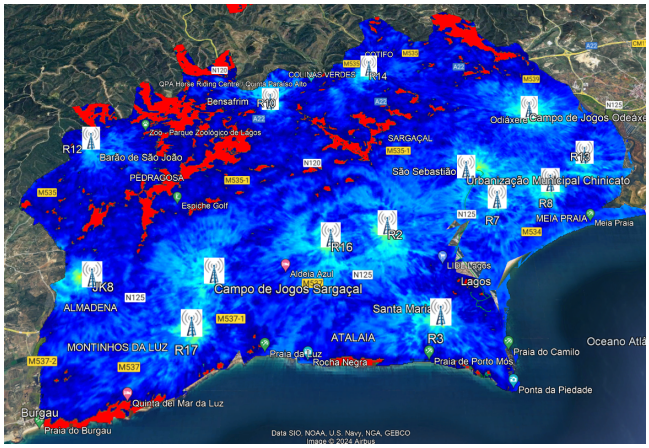

Figure 3: Municipality Area LoRAWAN Coverage

A Network performance evaluation on LoRaWAN server-based Docker containers was addressed by Gerda Iswari et al [17] to collect and analyze data, presenting a web application deployment process and container implementation. Results show that the web application on a container environment can display data in real-time and isolate applications without affecting other applications with high performance being able to handle requests up to 460 users without errors and good latency up to 300 users.

In Section 4 the secure LoRaWAN architecture and infrastructure is presented, where the implementation was based on the best practices described on the related work

4 Secure LoRaWAN Architecture and Infrastructure

As previously presented, LoRaWAN uses security in three distinct areas, authentication, integrity protection and confidentiality, combining AES with CMAC and CTR. In the related work, several approaches have been addressed to outperform LoRaWAN security. This work intents to present an distinct LoRaWAN architecture and infrastructure approach to secure data and communication.

The LoRaWAN network infrastructure implementation in Lagos Municipality has fourteen gateways (Figure 1), most of them connected through fiber optic direly in a star topology to the Municipality internal network and all of them are able to also communicate over 4G/5G with fixed IP addresses for communication redundancy.

The total area coverage rounds 95% as shown is Figure 3, where the red represents the not covered areas and blue the covered areas. The most populated areas are fully covered, considering that most of the smart things are to be implemented in this areas.

In a LoRaWAN network, there are three things that should be secured, the smart device itself in where the DevAddr, AppSKey and NwkSKey for communication are stored. The default password

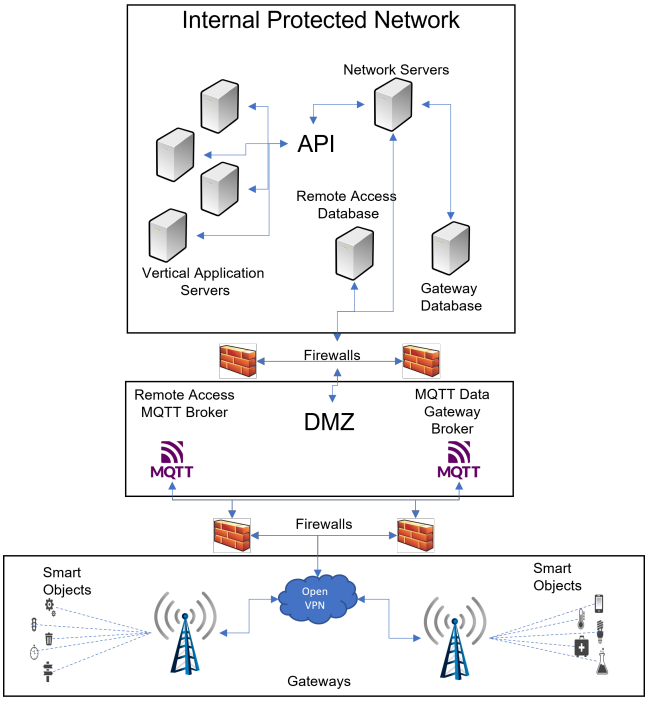

Figure 4: Secure LoRaWan Architecture

to remotely access the device, must be altered with a strong and distinct password. This is important because there are smart devices that perform actions and can be triggered remotely. If someone with bad intentions could access and activate an action on the smart device could trigger and damage something important.

The second thing to be secured is the communication between devices and gateways and the redirection to the Network and Remote Access Servers. The communication must be encrypted between devices and gateways and there should be Brokers instead of Network Servers on a DMZ to communicate with the gateways. If the Brokers are compromised, the data and monitoring will still be available, because the Network and Remote Access Servers are not exposed on the DMZ and are protected inside the Internal Network.

The third and last thing that has to be secured is the Internal Protected Network, where all data arriving from the MQTT Brokers is verified and only some communication ports are allowed using the Municipality firewalls.

In Figure 4 the architecture infrastructure is presented. There are three distinct layers, representing the three different refereed things to secure, the first, a physical layer where smart objects connect to the LoRaWAN gateways and the communication between gateways and firewalls, is established using an open VPN for each of the 14 gateways. The Open VPN assures that all traffic between gateways and brokers is encrypted on top of the encryption already performed by the LoRaWAN protocols previously presented, protecting this way MQTT packets from being altered. This way, it is implemented on top of the LoRaWAN 128-bit AES encryption communication a 256-Bit AES encryption, enforcing security and being able to communicate only the gateways that are set in the Firewalls configuration with the AES keys defined on both ends, due to its symmetric features. The Gateways receive packets from the smart devices and only are redirected if the device is authorized and already been activated, confirming if the device is registered in the remote access database, using a remote access MQTT broker and both NwkSKey and AppSkey randomly generated from 128-bit AES implemented on the LoRaWAN network.

The second layer is a Demilitarized Zone (DMZ), where only the MQTT brokers are exposed. Packets that arrive in both redundant firewalls are filtered, allowing only traffic originated from the gateways IP addresses and from the defined TCP ports and allowed by the firewalls rules. The remote access MQTT Broker confirms if the device is registered and activated and then allows the connection establishment to the MQTT data Gateway broker to receive the data from the smart devices. This way, only MQTT packets from specific TCP ports and from the specific Gateways IPs are able to be redirected to the Network Server and data is stored in the Gateway Database.

The third layer is on a restricted internal protected network, allowing only the exact needed ports, filtered by the firewalls, to connect from the DMZ to the Network Servers and from them to the Gateway Database, where data is stored. In this layer, the communication establishment between vertical application servers and the connected Network Server API, allowing data retrieval for monitorization, action, vertical management and statistics in each distinct area.

In the infrastructure, containers were used due to the isolation capacity and to facilitate the container deployment. All MQTT Brokers, Network Servers, Remote Access Database and Gateway database were deployed in containers using Docker. In case of attack, communications pass through the firewall, as explained in the related work, hardening the communications and preventing network attacks. If the MQTT brokers, in the DMZ layer of the architecture, which are exposed to the internet with external IP addresses, are compromised, Docker Container technology capacities makes it very easy to redeploy the containers and diminishing the solution downtime. Nevertheless, it is very important to harden the security communication to the Brokers, and to mitigate, as previously explained, all communications are filtered though the firewalls.

Adding security on a architecture usually increases time and processing, diminishing performance. In this case, a comparison between LoRaWAN (Figure 2) standard implementation and the secured architecture and infrastructure was done. A medium time for a packet to reach the network server from a gateway did not increase substantially, but the number of smart objects are still reduced, around 3200 and the servers have few processing needs. Only in time, with an increasing number of smart objects implemented, a complete study can be addressed to understand if the performance decreases substantially and what can be done to improve the communication.

This architecture and infrastructure approach allows better security on top of the default LoRaWAN security with a improved end-to-end secure communication.

5 Secure Communications

In order to enhance security in the MQTT Servers, Transport Layer Security (TLS) protocol was enabled increasing encryption and securing the communication between the MQTT Clients, the MQTT brokers and the servers, Network Servers and the Remote Access Database Server, preventing, therefore, possible unauthorized accesses or data interception.

Digital certificates were used to ensure only authorized clients can connect to the MQTT Servers, imposing also strong passwords to client authentication and administrative accesses to the MQTT servers. The firewalls only allow the service ports to be connected, intrusion detection and protection were also enabled and logging mechanisms were implemented to register and analyze MQTT servers activities.

The connections between the DMZ and Internal Protected Network are also verified by the firewalls to allow only the exact ports and IP addresses to connect and let pass the MQTT packets.

6 Resilient and Security Tests

The architecture and infrastructure is now being tested by security personal of the Lagos Municipality in Portugal, where several tests have been applied. Tests like Man-in-the-Middle using a rogue gateway, Replay attack exploiting a join request while jamming the original sender, Bit-Flipping attack injecting fake messages by modifying the payload, DOS with radio frequency jamming attack have been performed and as far, unsuccessful.

Several other tests are being prepared to be enforced on the architecture and infrastructure to test the resiliency and integrity.

7 Conclusions and Future Work

The main objective of this paper was to present, as far as known, a distinct secure architecture and infrastructure able to secure communications and data originated from the smart devices on a LoRaWAN network. To ensure security, several layers were created, physical layer where all smart devices have a secure and strong remote access password and the random generated keys from the LoRaWAN implementation to secure device discovery, activation and registration. A redundant firewall was implemented to secure the communications between Gateways and Brokers and on top a VPN to ensure a stronger packet redirection from the Municipality Gateways and not from rogue ones. Only the IP addresses and needed TCP ports on that communication are open.

The Broker servers are on a DMZ where the input and output communication are verified and filtered by the firewalls, securing all communication from DMZ into the Secure Internal Protected Network and from the outside external unprotected network. Only the brokers are allowed to be visible on the internet and only the communication from the Municipality Gateways is allowed.

Docker containers were used for the infrastructure, improving isolation and easy deploy, making the infrastructure more resilient and easy to manage.

For future work, it is intended to expand the number of smart devices and vertical applications to maximize the implemented LoRaWAN network. With the increasing number of smart devices, more data will be generated and it will be possible to apprehend better the secure architecture and infrastructure performance and be able to apply other security measures or improve the infrastructure. Other studies over the gathered data can also be applied.

Acknowledgments

This work is supported by NOVA LINCS ref. UIDB/04516/2020 (https://doi.org/10.54499/UIDB/04516/2020) and ref. UIDP/ 04516/2020 (https://doi.org/10.54499/UIDP/04516/2020) with the financial support of FCT.IP.

This work was also supported by Instituto Superior de Engenharia (ISE) from Universidade do Algarve.

References

[1] Samira Abboud and Nabil Abdoun. 2024. Enhancing LoRaWAN Security: An Advanced AES-Based Cryptographic Approach. *IEEE Access* 12 (2024), 2589–2606. https://doi.org/10.1109/access.2023.3348416

[2] LoRa Alliance. 2017. LoRaWAN Security,Full End-to-End Encryption for IoT Application Providers, White Paper.

[3] Dinda Wahyu Anggraeni, Muhammad Ary Murti, and Nachwan Mufti Adriansyah. 2023. Network Planning for Smart Water Metering Using LoRaWAN: Study Case for PDAM in Banyumas Regency. In *2023 9th International Conference on Wireless and Telematics (ICWT)*. IEEE. https://doi.org/10.1109/icwt58823.2023.10335431

[4] Alfredo Arnaud, María Eugenia Araújo, Ariel Dagnino, Joel Gak, Aarón Jimenz, José Job Flores, Matías Miguez, and Luis Arturo Soriano. 2023. A Model for a Dense LoRaWAN Network in the Agribusiness. In *2023 IEEE Conference on Agri-Food Electronics (CAFE)*. IEEE. https://doi.org/10.1109/cafe58535.2023.10291369

[5] Philippe Bogaerts. 2017. ARP Spoofing Docker Containers.

[6] Mi Chen, Lynda Mokdad, and Jalel Ben Othman. 2023. Robustness and Resilience of LoRaWAN Facing Greedy Behaviors on the MAC Layer. In *ICC 2023 - IEEE International Conference on Communications*. IEEE. https://doi.org/10.1109/icc45041.2023.10278996

[7] Mi Chen, Jalel Ben Othman, and Lynda Mokdad. 2023. Intelligent Urban Expressway Managing Architecture Using LoRaWAN and Edge Computing. In *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*. IEEE. https://doi.org/10.1109/globecom54140.2023.10436733

[8] LoRa Alliance Technical Committee. 2020. Lorawan l2 1.0. 4 specification (ts001-1.0. 4). Online. https://resources.lora-alliance.org/technical-specifications/ts001-1-0-4-lorawan-l2-1-0-4-specification

[9] LoRa Alliance Technical Committee. 2021. RP002-1.0.3 LoRaWAN Regional Parameters. https://lora-alliance.org/wp-content/uploads/2021/05/RP002-1.0.3-FINAL-1.pdf

[10] LoRa Alliance Technical Committee. 2022. Lora Alliance lorawan and 5g infographic. (2022). https://resources.lora-alliance.org/infographic

[11] Arrizky Ayu Faradila Purnama and Muhammad Imam Nashiruddin. 2019. Designing LoRaWAN Internet of Things Network for Advanced Metering Infrastructure (AMI) in Surabaya and Its Surrounding Cities. In *2019 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*. IEEE. https://doi.org/10.1109/isriti48646.2019.9034571

[12] Joel Guerreiro, Luis Rodrigues, and Noelia Correia. 2020. *On the Allocation of Resources in Sensor Clouds Under the Se-aaS Paradigm*. Springer International Publishing, 544–556. https://doi.org/10.1007/978-3-030-49108-6_39

[13] Yacoub Hanna, Mumin Cebe, Juan Leon, and Kemal Akkaya. 2024. Efficient Group Key Management for Resilient Operation of LoRaWAN-Based Smart Grid Applications. *IEEE Transactions on Control Systems Technology* (2024), 1–12. https://doi.org/10.1109/tcst.2024.3378988

[14] Vojtech Hauser and Tomas Hegr. 2017. Proposal of Adaptive Data Rate Algorithm for LoRaWAN-Based Infrastructure. In *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud)*. IEEE. https://doi.org/10.1109/ficloud.2017.47

[15] Ningning Hou, Xianjin Xia, and Yuanqing Zheng. 2021. Jamming of LoRa PHY and Countermeasure. In *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*. IEEE. https://doi.org/10.1109/infocom42981.2021.9488774

[16] Siti Nur Ilmani Binti Mohd Yusoff and Yusnani Binti Mohd Yussoff. 2022. Analysis of Security Vulnerabilities in LoRaWAN Smart City. In *2022 IEEE Symposium on Wireless Technology & Applications (ISWTA)*. IEEE. https://doi.org/10.1109/iswta55313.2022.9942752

[17] Gerda Iswari, Rahardhita Widyatra Sudibyo, Haryadi Amran Darwito, and Md. Manowarul Islam. 2021. Network Performance Evaluation of Container Server-based LoRaWAN IoT for Field Worker Monitoring System. In *2021 International Electronics Symposium (IES)*. IEEE. https://doi.org/10.1109/ies53407.2021.9593948

[18] Sneha K, Jayanth Reddy S, Surya Prakash B, and Ganesh P. 2023. IoT Based Smart Helmet for Workers in Mines Using LoraWAN. In *2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN)*. IEEE. https://doi.org/10.1109/vitecon58111.2023.10157165

[19] Sokratis Katsoulis, Christos Oikonomidis, Vasileios Angelopoulos, Dimitris Karampatzakis, and Thomas Lagkas. 2024. A LoRaWAN Vibration Detection Sensor for IoT Applications. In *2024 Panhellenic Conference on Electronics; Telecommunications (PACET)*. IEEE. https://doi.org/10.1109/pacet60398.2024.10497014

[20] Alexandru Lavric and Adrian Ioan Petrariu. 2018. LoRaWAN communication protocol: The new era of IoT. In *2018 International Conference on Development and Application Systems (DAS)*. IEEE. https://doi.org/10.1109/daas.2018.8396074

[21] Alexandru Lavric and Valentin Popa. 2017. Internet of Things and LoRa™ Low-Power Wide-Area Networks: A survey. In *2017 International Symposium on Signals, Circuits and Systems (ISSCS)*. IEEE. https://doi.org/10.1109/isscs.2017.8034915

[22] Luz E. Marquez, Alfonso Osorio, Maria Calle, Juan C. Velez, Antonio Serrano, and John E. Candelo-Becerra. 2020. On the Use of LoRaWAN in Smart Cities: A Study With Blocking Interference. *IEEE Internet of Things Journal* 7, 4 (April 2020), 2806–2815. https://doi.org/10.1109/jiot.2019.2962976

[23] A. Martin, S. Raponi, T. Combe, and R. Di Pietro. 2018. Docker ecosystem – Vulnerability Analysis. *Computer Communications* 122 (June 2018), 30–43. https://doi.org/10.1016/j.comcom.2018.03.011

[24] Asem Mousa, Wajeeh Tuffaha, Mohammad Abdulhaq, Moath Qadry, and Othman Othman M.M. 2023. In-Depth Network Security for Docker Containers. In *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. IEEE. https://doi.org/10.1109/icccnt56998.2023.10307493

[25] Drake Mubanda, Ngaira Mandela, Tumaini Mbinda, and Christopher Ayesiga. 2023. Evaluating Docker Container Security through Penetration Testing: A Smart Computer Security. In *2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI)*. IEEE. https://doi.org/10.1109/iccsai59793.2023.10421124

[26] Muhammad Aamir Nashrullah, Pradini Puspitaningayu, Muhamad Bagus Fikril Alan, Erwin Sutanto, Fahmi Fahmi, and Unit Three Kartini. 2024. An Evaluation of LoRaWAN and WLAN for IoT-based Photovoltaic Microgrid Monitoring. In *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*. IEEE. https://doi.org/10.1109/icetsis61505.2024.10459411

[27] Jorge Navarro-Ortiz, Natalia Chinchilla-Romero, Juan J. Ramos-Munoz, and Pablo Munoz-Luengo. 2019. Improving Hardware Security for LoRaWAN. In *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE. https://doi.org/10.1109/cscn.2019.8931397

[28] Lorenzo Parri, Stefano Parrino, Giacomo Peruzzi, and Alessandro Pozzebon. 2020. A LoRaWAN Network Infrastructure for the Remote Monitoring of Offshore Sea Farms. In *2020 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*. IEEE. https://doi.org/10.1109/i2mtc43012.2020.9128370

[29] Olivier Seller. 2021. LoRaWAN Security. *Journal of ICT Standardization* (April 2021). https://doi.org/10.13052/jicts2245-800x.915

[30] Mattia Giovanni Spina, Mauro Tropea, and Floriano De Rango. 2024. Securing MQTT-M2M Communications in a Food Retail Distribution. In *2024 IEEE 21st Consumer Communications; Networking Conference (CCNC)*. IEEE. https://doi.org/10.1109/ccnc51664.2024.10454863

[31] Sari Sultan, Imtiaz Ahmad, and Tassos Dimitriou. 2019. Container Security: Issues, Challenges, and the Road Ahead. *IEEE Access* 7 (2019), 52976–52996. https://doi.org/10.1109/access.2019.2911732

[32] Kun Suo, Yong Zhao, Wei Chen, and Jia Rao. 2018. An Analysis and Empirical Study of Container Networks. In *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*. IEEE. https://doi.org/10.1109/infocom.2018.8485865

[33] Chin-Wei Tien, Tse-Yung Huang, Chia-Wei Tien, Ting-Chun Huang, and Sy-Yen Kuo. 2019. KubAnomaly: Anomaly detection for the Docker orchestration platform with neural network approaches. *Engineering Reports* 1, 5 (Dec. 2019). https://doi.org/10.1002/eng2.12080

[34] Rahul Tomar and Olaf-Gerd Gemein. 2018. LoRa network for cities Private and complete secured by design. In *2018 Global Internet of Things Summit (GIoTS)*. IEEE. https://doi.org/10.1109/giots.2018.8534557

[35] Nikolaos Tsavalos and Ahmad Abu Hashem. 2018. Low Power Wide Area Network (LPWAN) Technologies for Industrial IoT Applications. (2018).

[36] Zhifu Zhang, Yucheng Liu, Gerhard P. Hancke, and Kim Fung Tsang. 2023. A Standardized Edge Computing Infrastructure of LoRaWAN Using IEEE 2668. In *2023 IEEE 21st International Conference on Industrial Informatics (INDIN)*. IEEE. https://doi.org/10.1109/indin51400.2023.10218036