Credential Lifecycle Analysis in Private LoRaWAN Networks for Industrial IoT (IIoT)

Sergio H. Silva[a], Guilherme P. Koslovski[b], Mauricio A. Pillon[c] and Charles C. Miers[d]
Graduate Program in Applied Computing (PPGCAP), Santa Catarina State University (UDESC), Brazil

Keywords: Industrial Internet of Things (IIoT), LoRaWAN, Access Control, Credentials Lifecycle.

Abstract: The adoption of smart devices in the industrial context has led to the emergence of the Industrial Internet, also known as the Industrial Internet of Things (IIoT). Compliance with security requirements and standards is necessary for IIoT networks, including general Internet technology standards and specific standards for IIoT regulation, such as those defined by the Industrial Internet Consortium (IIC). In this article, we focus on the issue of non-compliance with the credential lifecycle in private LPWAN LoRaWAN networks based on ChirpStack, a widely used open-source solution for connecting IoT devices over large geographical areas. Non-compliance with credential lifecycle standards can pose risks to business continuity. Our goal is to analyze the lifecycle of credentials in the context of IIoT using the LoRaWAN 1.1 protocol with ChirpStack servers. The contributions of this work include identifying the lifecycle of identities applied and analyzing the identity lifecycle when used with ChirpStack open-source LoRaWAN Network Server.

1 INTRODUCTION

The adoption of smart devices in the industrial context resulted in the so-called Industrial Internet, or Industrial Internet of Things (IIoT). The incorporation of smart devices in industrial complex and critical scenarios has several security requirements, application areas, and others (De Sousa et al., 2019). Access control and identity management are the main ways to guarantee the authenticity of devices in all computational contexts. In this critical context, the need to adhere to security requirements and policies (Kobara, 2016). IIoT network arrangements must comply to general Internet technology standards. In addition, it must observe the standards of specific entities for IIoT regulation such as the Industrial Internet Consortium (IIC). IIC defines IIoT architecture, data analytics, connectivity, and security. Furthermore, IIC assigned standards comply with the referential standards (NIST, ISO, and IEEE). The standards include security recommendations related to IIoT access control and credential lifecycle (Schrecker et al., 2016).

Low Power Wide Area Network (LPWAN) networks are used in industrial contexts in which the requirements are of wide area with energy restrains (Luvisotto et al., 2018). LoRaWAN is a LoRa-based protocol very popular and widely used by organizations to connect several IoT devices deployed on a large geographical area. This implementation is often performed with a private LoRaWAN network arrangement using ChirpStack servers (Yu et al., 2022). These private LoRaWAN networks using ChirpStack servers may include new security vulnerabilities in an industrial environment.

Networks not complying IIC standards related to identity management and credential lifecycle may pose a risk for business continuity. We focus on the issue of non-compliance of the credentials lifecycle in the context of private LPWAN LoRaWAN private networks based on ChirpStack. Moreover, we analyze the lifecycle of credentials, identifying conformities and problems related to the various existing identities/credentials in an IIoT LoRaWAN ChirpStack system. Our main contributions are: (i) identification of the lifecycle of identities applied to LoRaWAN 1.1; and (ii) identification and analysis of the identity lifecycle in LoRaWAN 1.1 based on ChirpStack.

This article is organized as follows. Section 2 introduces basic concepts. Section 3 presents the problem. Section 4 summarizes related works. Section 5

[a] https://orcid.org/0000-0003-4923-189X
[b] https://orcid.org/0000-0003-4936-1619
[c] https://orcid.org/0000-0001-7634-6823
[d] https://orcid.org/0000-0002-1976-0478

Silva, S., Koslovski, G., Pillon, M. and Miers, C.
Credential Lifecycle Analysis in Private LoRaWAN Networks for Industrial IoT (IIoT).
DOI: 10.5220/0012615500003705

In *Proceedings of the 9th International Conference on Internet of Things, Big Data and Security (IoTBDS 2024)*, pages 157-165
ISBN: 978-989-758-699-6; ISSN: 2184-4976

presents our proposal and criteria. Finally, the Section 6 presents our analysis and mitigation proposal.

2 FUNDAMENTALS

Like any computing arrangement, the IIoT needs to ensure security when it comes to access control. A central piece in access control is authentication and authorization. In device authentication, credentials are widely used to recognize these entities (Kim and Lee, 2017). According to (Schrecker et al., 2016), the definition of credential refers to evidence that supports a claim of identity or an attribute. This definition complies with the standardization described in revision number 4009 of the Committee on National Security Systems (CNSS) glossary. The credentials lifecycle in a computing environment must also comply with standards and best practices. The security and identity management standard endorsed by the IIC has registration, management, and authentication phases – Figure 1 (Schrecker et al., 2016).

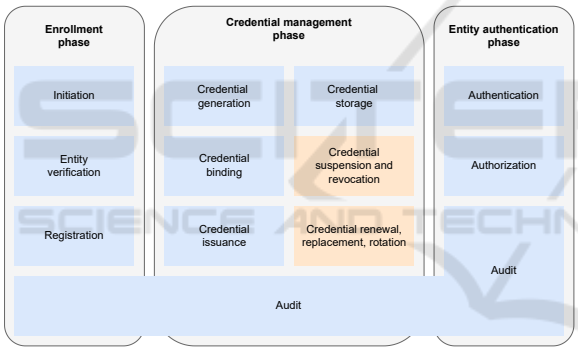

Figure 1: IIoT identity management lifecycle.

Figure 1 shows the recommended lifecycle consists of three phases which in turn contain several steps. The presented cycle serves as an analysis parameter in the analysis scenario of this work. In this article, the definition of IIoT is interpreted, based on (Lin et al., 2017), i.e., as a system in which there is the connection and integration of industrial infrastructure and end devices. Thus, relying on a network and control infrastructure to enable data analysis and visualization, in addition to centralized control by high-level business systems (Figure 2).

The Edge Layer contains the devices which needs to be identified in addition to the edge gateways are found. This layer usually has devices in wireless networks that can use different protocols or technologies (Gulati et al., 2022). The Platform Layer includes the network and application servers, and is responsible for storing, transporting, and transforming data.

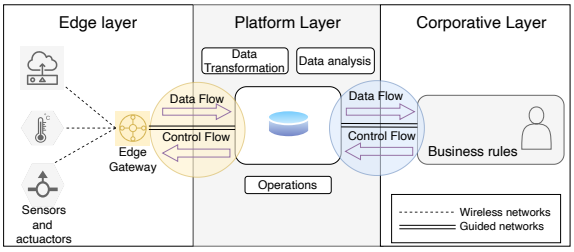

Figure 2: IIoT referential architecture.

The Corporative Layer is where business operations are carried out. From this layer originates the control flow of the entire IIoT system. The data flow originates in the edge layer, passing through the platform layer to the enterprise layer. Our work bases the studies on this referential architecture. In which the technology used for the transmission of the devices to the gateways is LoRaWAN, based on the LoRa protocol. This technology and protocol were chosen based on cost, area, and availability of open server software. However, there are two version of LoRaWAN protocol being currently used: 1.0 and 1.1 (Table 1).

Table 1: LoRaWAN security comparison: 1.0 vs. 1.1.

	LoRaWAN 1.0	**LoRaWAN 1.1**
Session Keys	AppSkey and NwkSkey	FNwkSIntKey, SNwkSIntKey, NwkSEncKey and AppSKey
MAC commands	Not encrypted	Encrypted
Entities	End Devices, Network Server and Application Server.	End Devices, Join Server, Network Server and Application Server
Roaming between LoRaWAN networks	Does not support roaming between networks	Supports roaming between networks
Entity responsible for the network server joining process	Network Server	Join Server
Reuse of counters	Do not persist counters, it may compromise cryptography and communication.	Corrected by storing the last value of the counter in non-volatile memory.
Repeat request message failed	An invader must wait for just N messages before playing a message requesting a connection.	The repetition of messages of the type join request is prevented by the network does not increase.
End-to-end	No protection from end to end. As the AppKey is shared by both the network server and the application servers, it is subject to interception.	End-to-end protection for OTAA is achieved by providing two different keys for the network (NwkKey) and for the application (AppKey), from which all other keys are derived.

The LoRaWAN protocol is defined by the Lora Alliance — a consortium of companies such as IBM, Actility, Semtech, and Microchip — as a networking protocol LPWAN was designed to connect battery-operated devices on a long-range wireless network. The LoRaWAN version 1.0 of was released in 2015, undergoing updates in the following years until its update to version 1.1 in 2017. We focus on version 1.1 as it is the most recent and recommended version for an environment with (Dönmez and Nigussie, 2018) security requirements.

3 PROBLEM

The development of the IIoT is surrounded by several challenges when it comes to its safe, stable, and profitable implementation for industrial organizations. These challenges are related to the implementation of a reference architecture and security policies based on norms and standards. Other use case characteristics of IIoT applications also bring additional considerations related to implementing a reliable and stable IIoT network. Our scenario is a layered architecture for IIoT with the use case of process automation and monitoring. This architectural pattern and end-use case result in an IIoT system with requirements for a wide distribution area of the end devices in the organization's physical space. In this work, under criteria of the low cost of end devices, long-range, energy saving, and flexibility, the LPWAN LoRaWAN protocol was chosen. In terms of LoRaWAN, some organizations require deployment as a private network, ensuring isolation from potential attackers. Furthermore, the environment used in the work procedures will use the ChirpStack software component to implement the protocol entities. Even though LoRaWAN with ChirpStack satisfies these requirements, the traditional approach to the protocol does not provide for a defined lifecycle for the credentials used to verify the authenticity of devices.

Given the proposed study scenario, there is a concern about how to safely manage IIoT devices requiring secure credentials. It also raises the question of how to implement the lifecycle recommended by IIoT standardization entities in LoRaWAN networks, which was not originally thought for the industrial scenario. In a scenario in which their quantity is significant, improper/malicious management of devices can cause authentic devices not to be well used and non-authentic devices to join the network. The consequences of not implementing an organized credentials lifecycle can compromise the system's security as a whole, opening the possibility of devices with compromised keys continuing to integrate the network and compromising the data sent to the business layer or even enabling attacks of interception of information.

The evaluation criteria to verify whether there are solutions to this problem in the literature should be based on basically four motivating questions: Q1: It proposes to use a lifecycle to ensure device access control security? Q2: It proposes a solution for managing credentials in environments with wide area requirements with remote configuration? Q3: It employs LPWAN LoRaWAN protocol in communication? Q4: Aimed at industrial contexts (IIoT)?

4 RELATED WORK

The selection of related works aimed to raise research related to the problem addressed, and, in this sense, we also sought to analyze trends regarding the proposed problems. This mapping also aimed to identify gaps in the number of publications on a given subject through the production of a structured classification. The keywords to identify works in academic search engines: `(Industrial Internet of Things OR IIoT) AND LoRaWAN AND (Control Access OR Identity Management OR lifecycle management)`.

The process of selecting papers was carried out in consideration of the recommendations arising from (Galvão et al., 2015). Search sources selected were IEEE Xplore, Science Direct, and Science.gov, due to their availability of features such as advanced filters and better data visualizations. Identified were submitted to the inclusion criteria (IC) and exclusion criteria (EC). ICs: **IC01**: published on the last decade (2012 - 2023); **IC02**: address access control in LoRaWAN networks for IoT / IIoT; **IC03**: focus on the management of identity and credentials of devices in LoRaWAN networks; and **IC04**: evaluate the authentication of industrial devices (IIoT). ECs: **EC01**: published in commercial or non-academic journals, or has not yet been reviewed; **EC02**: published more than a decade ago, that is, it is before 2012; **EC03**: do not address, or only indirectly addresses, the issue of credential management in LoRaWAN; and **EC04**: do not address, or indirectly addresses, the use of IoT / IIoT devices. Figure 3 shows from the initial identification of works in the ASEs to the final synthesis.

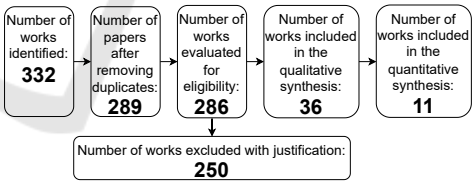

Figure 3: Related work evaluation process.

According to Figure 3, the works went through a filter to remove duplicate works and, subsequently, were submitted to an eligibility assessment according to the inclusion and exclusion criteria. Then, the works were included in a qualitative synthesis, whose summary content and main topics of the publication were evaluated. Thus, the number of papers included in the final quantitative synthesis was arrived at. Table 2 reveals there were no works meeting all requirements from our research problem.

Table 2: Related works identified.

	Q1: Propose lifecycle of credentials?	Q2: Requirements for wide area and configuration remote?	Q3: Uses networks LPWAN and protocol LoRaWAN?	Q4: Is aimed at industrial scenarios IIoT?
(Ribeiro et al., 2020)	Yes	No	Yes	No
(Sanchez-Iborra et al., 2018)	Yes	No	Yes	No
(Naoui et al., 2016)	Yes	No	Yes	No
(Ralambotiana, 2018)	Yes	No	Yes	No
(McPherson and Irvine, 2020)	Yes	Yes	Yes	No
(e Margaret Lech e Liuping Wang, 2021)	Yes	Yes	Yes	No
(Naoui et al., 2017)	No	No	Yes	Yes
(Xing et al., 2019)	Yes	No	Yes	No
(Sanchez-Gomez et al., 2020)	Yes	Yes	No	No
(Felli and Giuliano, 2021)	Yes	Yes	Yes	No

5 PROPOSAL

The proposal consists of an analysis of the lifecycle of credentials for private networks of LPWAN networks, implemented with the LoRaWAN protocol with servers using the ChirpStack component. Our scenario is based on a layered architecture for IIoT, based on the proposal of (Lin et al., 2017).

In the LoRaWAN context, the final device provides credentials for the join procedure process. The binding step between the credential and the Identity and Access Management (IAM) entity is performed in an operation between the edge and platform layer in the join procedure before sending the join accept message. Credentials are issued and stored in the platform layer of the referential architecture, which is responsible for infrastructure and network operations. Regarding the LoRaWAN protocol, the entities involved are the Join Server and the network server, and operations are performed after the join procedure. The credential suspension and revocation is an operation involving two layers of the architecture: the platform and the enterprise layer. In parallel, in LoRaWAN, this operation can be triggered by the Join Server or the LoRaWAN application server through control systems.

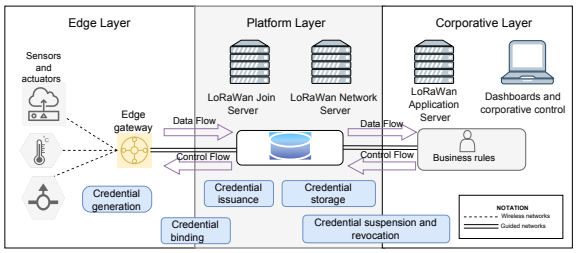

Figure 4: Proposal architecture.

Figure 4 shows the generic reference architecture of IIoT can serve as a framework for LoRaWAN networks in the industrial context. This analysis scenario is justified by requirements on IIoT services. Implementing LoRaWAN networks is directly linked to the use case requirements, number of devices, and typical service area as per (Brown et al., 2018). At the same time, using components for ChirpStack for LoRaWAN servers is justified by being widely used, having the most significant active community, and having periodic and current updates (Lund, 2022).

The application domain of the proposal can be defined as an industrial context with a large service area, low power availability, and remote management. Thus, the correct security management in the scenario of this proposal takes to our problem (Section 3).

5.1 Testbed

The experimentation environment employs GNU/Linux Ubuntu Server version 22.04 operating system. The architecture components are simulated as depicted in Figure 4. The Edge Layer features simulated end devices, specifically temperature gauges, and the simulated LoRaWAN gateway. All components were configured in a ChirpStack version 3.16.3 ecosystem, these components are equivalent to factory floor end devices in the industrial scenario, and the gateway is equivalent to a physical gateway. These components are simulated on a computer with hardware integrated by an Intel Core I3 64bit processor, 8GB of DDR4 memory, and a 1TB hard drive. The servers are installed under an Apache web server and Postgresql Server database directly on the native operating system. At the Platform Layer, the environment has a network server and a join server, LoRaWAN 1.1, both implemented by the ChirpStack ecosystem. The network server and the join server are the same used in real environments and similar to those used in a real factory environment. The application server and the Application Programming Interface (API) also from ChirpStack are used in the Enterprise Layer. The application server and the programming interface are identical to those used in the real world. API management is performed by the Insomnia API client (Information at: https://insomnia.rest/, in version 2022.2.1. Detailing the experimentation environment guarantees the reproducibility of the experiments. Thus, it is possible to detail the testbed architecture and the test plan related to the analysis.

5.2 Method of Analysis

The primary purpose of this research is to carry out a lifecycle analysis of credentials in LPWAN LoRaWAN 1.1 networks according to the recommended standards for IIoT. We defined criteria (C) employed in our tests and experiments to allow our analysis and

indicate possible solutions for the identified problems. Each criterion is based on identity management standards: **(C1)** - Credential lifecycle phases: Identify the credential lifecycle phases of a LoRaWAN network deployed with ChirpStack servers for IIoT. We verify that the procedures are categorized into registration, management, and authentication phases. **(C2)** - Credential lifecycle phases: Identify which phases are involved in the LoRaWAN ChirpStack context identity lifecycle phases. The registration phase should contain initiation, verification, and entity registration steps. The management phase must add the generation, binding, issuance, and storage of credentials. In addition, the management phase should cover contingency measures such as suspension, renewal, and replacement of credentials. **(C3)** - Audit mechanisms: Verify the audit mechanisms in the LoRaWAN ChirpStack context in the credential lifecycle. The audit process is a step present in all phases of the lifecycle. It is evaluated whether the audit in this scenario goes beyond these phases.

5.3 Environment Setup

The approach was chosen because it allows the implementation of a LoRaWAN architecture in a local, controlled environment with reduced cost and use of resources. The architecture has the essential components of a LoRaWAN network: end devices, join server, network server, and application server. The infrastructure components are implemented by a ChirpStack environment. The end devices and gateways are simulations that interact with a Network Server, a Join Server, and a conventional Application Server installed on a local server (Figure 5).

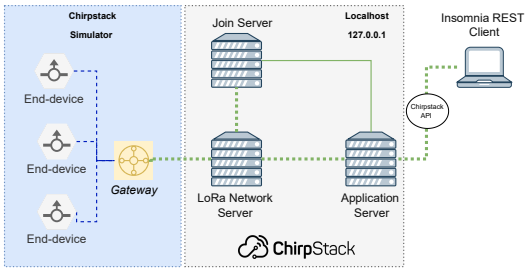

Figure 5: Overview of the experiment setup.

The LoRaWAN ChirpStack Network Server (https://github.com/brocaar/chirpstack-simulator was deployed to simulate devices and gateways, allowing to have a configurable number of devices and gateways, which can be automatically created when starting the simulation. In these tests, the server is initialized and has a simulation duration configured. It is possible to read the metrics and complete the simulation in the sequence. After this duration, the simulator can be terminated, and the created devices, gateways, applications, and device profiles are restarted. The interfaces of the application server and the API of ChirpStack were used to visualize and manage the devices and collect data. This does not interfere with the relationship with a real scenario, as it is strictly the same as operating in a production environment. The test plan was designed to synthesize the information related to the tests of this work. We reinforced that the analysis criteria are all analyzed in this test environment in their respective scenarios (Table 3).

Table 3: Consolidated test scenarios.

Phase	Step	Analysis criteria	Scenario	HTTP Request	Endpoint of ChirpStack API
Enrollment	Initiation	C1 and C2	Scenario 1	POST	/api/devices
Enrollment	Verification	C1 and C2	Scenario 1	POST	/api/devices
Enrollment	Registry	C1 and C2	Scenario 1	POST	/api/devices
Credential management	Generation	C1 and C2	Scenario 2	POST	/api/devices/{device_keys.dev_eui}/keys
Credential management	Vinculation	C1 and C2	Scenario 2	POST	/api/devices/{device_keys.dev_eui}/keys
Credential management	Issuance	C1 and C2	Scenario 2	POST	/api/devices/{device_keys.dev_eui}/keys
Credential management	Storage	C1 and C2	Scenario 2	GET	/api/devices/{dev_eui}/keys
Credential management	Renew, replacement and rotation.	C1 and C2	Scenario 3	PUT	/api/devices/{device_keys.dev_eui}/keys
Credential management	Suspention and revocation	C1 and C2	Scenario 3	DELETE	/api/devices/{dev_eui}/keys
Entity authentication	Authentication	C1 and C2	Scenario 4	POST	/api/devices/{device_activation.dev_eui}/activate
Entity authentication	Authorization	C1 and C2	Scenario 4	POST	/api/devices/{device_activation.dev_eui}/activate
Entity authentication	Audit	C3	Scenario 5	GET	/api/devices/{dev_eui}/events

6 RESULTS AND ANALYSIS

Each of these experiments analyzes a group of steps in a phase of the lifecycle of credentials described in the work's rationale. Each experiment scenario starts with a definition of objectives and the related scope. Thus, the scope is relative to the steps and phases analyzed. As well as carried out individually in each scenario, a global analysis of the scenarios was carried out. The definition of scenarios and experiments, as well as the attributes that are part of the execution of the tests, are described in Table 4 and Figure 6.

Table 4: Test results consolidation.

Test Scenarios	Experiment	Execution code	Credentias involved	Requirements compliance	Analysis Criteria	Results
Scenario 1	Experiment 1	Code 1 Code 2	devEUI	Fully fulfilled	Criterion 1	The operation performs the steps of initiation, verification and registration.
Scenario 2	Experiment 1	Code 3 Code 4	devEUI, appKey, nwkKey, genAppKey	Fully fulfilled	Criterion 1	The operation executes generation, binding, issuance and store phases.
					Criterion 2	The operation performs generation, binding, issuance, and storage steps.
Scenario 3	Experiment 1	Code 5 Code 6	devEUI, appKey, nwkKey, genAppKey	Partially fulfilled	Criterion 1	The operation performs the renew and replace steps. Do not perform the rotation step.
					Criterion 2	The operation performs the credential management phase.
	Experiment 2	Code 7	devEUI, appKey, nwkKey, genAppKey	Partially fulfilled	Criterion 1	The operation performs the suspend step. Does not perform the revocation step.
					Criterion 2	The operation performs the credential management phase partially.
Scenario 4	Experiment 1	Code 8 Code 9	appSKey, devAddr, devEUI, fNwkSIntKey, nFCntDow, nwkSEncKey, sNwkSIntKey	Fully fulfilled	Criterion 1	The operation performs the authentication and authorization steps.
					Criterion 2	The operation performs the authentication phase.
Scenario 5	Experiment 1	Code 10	devEUI	Not fullfilled	Criterion 3	The operation does not perform an audit step in any of the credential lifecycle phases.

Table 4 groups the tests by test scenarios. Each scenario has experiments that use code to perform test operations. For each experiment, the LoRaWAN protocol credentials involved are listed. In addition, each experiment is analyzed through the prism of the anal-

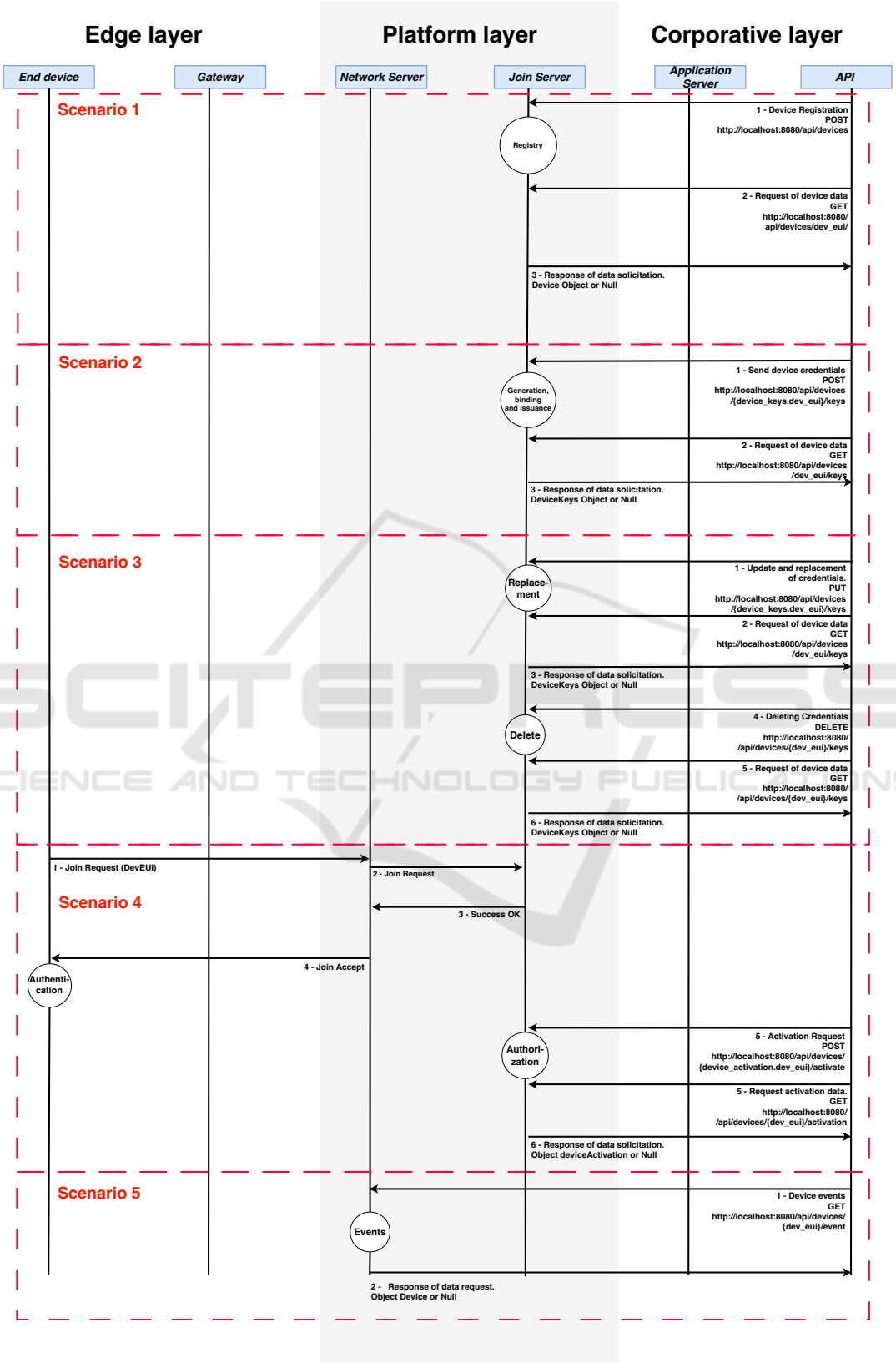

Figure 6: Sequence diagram of experiments.

ysis criteria.

Scenario 1 aims to test the initiation, verification, and registration steps in the registration phase. The credential involved in the test is the devEUI. This scenario had the analysis requirements fully met. Therefore, this test ensures that the scenario executes the steps and the analyzed phase, contributing to the results to attest that the test environment complies with the standards.

Scenario 2 aimed to test the generation, binding, issuance, and storage in the credential management step. We have devEUI, appKey, nwkKey, and genAppKey credentials involved in this test. The requirements were fully met, which adds to the result's proven suitability of the environment for the lifecycle and adequacy to the phases of generation, binding, issuance, and storage and to the credential management phase.

Scenario 3 has two experiments. In the first, the LoRaWAN credentials used are devEUI, appKey, nwkKey, and genAppKey. In this experiment, the requirements were fulfilled only partially because the application server does not have a rotation step. Thus, adding to the overall result, the point of attention is that the LoRaWAN protocol implemented by ChirpStack has dissonance with the lifecycle pattern. Still, the scenario understands renovation and replacement, so it partially lives up to the requirements.

In Scenario 3 and Experiment 2, the credentials devEUI, appKey, nwkKey, and genAppKey are used, and the requirements are only partially fulfilled. This is since the environment does not have the credential lifecycle revocation step. This is part of the overall analysis with the finding that the credential management phase is compromised in terms of revocation.

Scenario 4 looks at the appSKey, devAddr, devEUI, fNwkSIntKey, nFCntDown, nwkSEncKey, and sNwkSIntKey credentials. In the analysis carried out, this scenario fits the criteria so that the authentication and authorization operations are performed. Consequently, the authentication phase is available satisfactorily, adding to the result that authentication and authorization operations exist and are available as part of the cycle. This is vital for the functioning of an authentication scheme, so this result was expected.

Scenario 5 uses the devEUI identification credential and does not meet the analyzed requirements. Criterion 3 is not achieved, implying there is no possibility of auditing the test environment and not fulfilling credential lifecycle standards requirements. Table 5 summarizes the results obtained categorized by phases and steps of the lifecycle.

Performing a general analysis of the credentials lifecycle in private networks for IIoT implemented with ChirpStack, our key remarks are:

Table 5: Summary of results.

Lifecycle phase	Lifecycle phase	Analysis Criteria	Scenario	Result obtained
Enrollment	Initiation	Criterion 1 Criterion 2	Scenario 1	Suitable for the lifecycle
Enrollment	Verification	Criterion 1 Criterion 2	Scenario 1	Suitable for the lifecycle
Enrollment	Enrollment	Criterion 1 Criterion 2	Scenario 1	Suitable for the lifecycle
Credential management	Generation	Criterion 1 Criterion 2	Scenario 2	Suitable for the lifecycle
Credential management	Issuance	Criterion 1 Criterion 2	Scenario 2	Suitable for the lifecycle
Credential management	Storage	Criterion 1 Criterion 2	Scenario 2	Suitable for the lifecycle
Credential management	Renew, replacement and renew.	Criterion 1 Criterion 2	Scenario 3	Partially suitable for the lifecycle
Credential management	Suspension and revocation.	Criterion 1 Criterion 2	Scenario 3	Partially suitable for the lifecycle
Entity authentication	Authentication	Criterion 1 Criterion 2	Scenario 4	Suitable for the lifecycle
Entity authentication	Authorization	Criterion 1 Criterion 2	Scenario 4	Suitable for the lifecycle
Entity authentication	Audit	Criterion 3	Scenario 5	Not Suitable for the lifecycle

- The environment fulfills the requirements related to the initialization, verification, and registration steps of the registration phase.
- The environment fulfills the requirements related to the generation, binding, issuance, and storage steps of the credentials management phase.
- The environment fulfills the requirements associated with the authentication and authorization steps in the authentication phase.
- The environment partially fulfills the requirements regarding the credentials management phase. Because it correctly implements the renewal and replacement steps but does not perform the rotation step.
- The environment partially fulfills the requirements regarding the credentials management phase. Because it correctly implements the suspension step but does not execute the revocation step.
- The environment only partially meets the audit step. Step that is present in all phases.

In this way, the present work attests that the private LoRaWAN networks implemented in ChirpStack are not entirely adequate to the standards established for the IIoT. Thus, our work analyzes this protocol and the ChirpStack server so that developers can be aware of this arrangement's risks and necessary improvements regarding the lifecycle of credentials in compliance with standards.

7 CONSIDERATIONS AND FUTURE WORK

The IIoT is a relatively well-established concept. Several standardization lead to a well-defined architecture following the standards bodies such as ISO, NIST, and IIC. Thus, recommendations on security and identity lifecycle guide the definition of objectives. The characterization is in accordance with the main regulatory institutions of the international market in the field of Industrial Internet. The path necessary to achieve the goal of analyzing the lifecycle of LoRaWAN credentials provided by ChirpStack. With the approach of joining and activation procedures in LoRaWAN, the steps and phases of the credential lifecycle were related to the protocol credentials. This intersectionality is an important characteristic of the contribution of this work. The most concrete importance of this work was to avoid information security incidents in industries due to vulnerabilities in the lifecycle of credentials.

It was possible to state that the LoRaWAN private networks provided by ChirpStack needs to be improved to secure credentials during its lifecycle. There are disparities between the recommended and implemented lifecycle, mainly in auditing. Additionally, this environment does not fully implement recommended lifecycle steps such as credential rotation and revocation. Thus, it allows the work to serve as a basis for deploying technologies such as LoRaWAN in a risk-conscious manner or that the implementation can provide the points at which this computational arrangement falls short regarding the credentials lifecycle.

Furthermore, this work points to future work. A more comprehensive and updated bibliographic survey in terms of IIoT could be carried out, as it contributes to the concept of IIoT. Another future work that comes naturally from this work would be to improve ChirpStack for a fully lifecycle-compliant credential lifecycle. Implementations aimed at tracking lifecycle operations are vital. Another future work is fix security problems such as storing clear credentials stored in the database used by ChirpStack.

ACKNOWLEDGMENTS

This work was funding by the National Council for Scientific and Technological Development (CNPq, grant 311245/2021-8), FAPESC, UDESC, and developed at LabP2D.

REFERENCES

Brown, G. et al. (2018). Ultra-reliable low-latency 5g for industrial automation. *Technol. Rep. Qualcomm*, 2:52065394.

De Sousa, P. H. F., Navar de Medeiros, M., Almeida, J. S., Reboucas Filho, P. P., de Albuquerque, V. H. C., et al. (2019). Intelligent incipient fault detection in wind turbines based on industrial iot environment. *Journal of Artificial Intelligence and Systems*, 1(1):1–19.

Dönmez, T. C. and Nigussie, E. (2018). Security of lorawan v1.1 in backward compatibility scenarios. *Procedia Computer Science*, 134:51–58. The 15th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2018) / The 13th International Conference on Future Networks and Communications (FNC-2018) / Affiliated Workshops.

e Margaret Lech e Liuping Wang, X. C. (2021). A complete key management scheme for lorawan v1.1 †. *Sensors (Basel, Switzerland)*, 21.

Felli, L. and Giuliano, R. (2021). Access control in woodland through blockchain and lorawan. In *2021 AEIT International Conference on Electrical and Electronic Technologies for Automotive (AEIT AUTOMOTIVE)*, pages 1–5.

Galvão, T. F., Pansani, T. d. S. A., and Harrad, D. (2015). Principais itens para relatar revisões sistemáticas e meta-análises: A recomendação prisma. *Epidemiologia e serviços de saúde*, 24:335–342.

Gulati, K., Boddu, R. S. K., Kapila, D., Bangare, S. L., Chandnani, N., and Saravanan, G. (2022). A review paper on wireless sensor network techniques in internet of things (iot). *Materials Today: Proceedings*, 51:161–165.

Kim, H. and Lee, E. A. (2017). Authentication and authorization for the internet of things. *IT Professional*, 19(5):27–33.

Kobara, K. (2016). Cyber physical security for industrial control systems and iot. *IEICE TRANSACTIONS on Information and Systems*, 99(4):787–795.

Lin, S.-W., Miller, B., Durand, J., Bleakley, G., Chigani, A., Martin, R., and Crawford, B. M. M. (2017). Industrial internet consortium (iic) - the industrial internet of things volume g1: Reference architecture.

Lund, F. (2022). Study of lorawan device and gateway setups: with chirpstack implementation.

Luvisotto, M., Tramarin, F., Vangelista, L., and Vitturi, S. (2018). On the use of lorawan for indoor industrial iot applications. *Wireless Communications and Mobile Computing*, 2018.

McPherson, R. and Irvine, J. (2020). Secure decentralised deployment of lorawan sensors. *IEEE Sensors Journal*, 21(1):725–732.

Naoui, S., Elhdhili, M. E., and Saidane, L. A. (2016). Enhancing the security of the iot lorawan architecture. In *2016 International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN)*, pages 1–7. IEEE.

Naoui, S., Elhdhili, M. E., and Saidane, L. A. (2017). Trusted third party based key management for enhanc-

ing lorawan security. In *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*, pages 1306–1313.

Ralambotiana, M. (2018). Key management with a trusted third party using lorawan protocol: A study case for e2e security.

Ribeiro, V., Holanda, R., Ramos, A., and Rodrigues, J. J. (2020). Enhancing key management in lorawan with permissioned blockchain. *Sensors*, 20(11):3068.

Sanchez-Gomez, J., Garcia Carrillo, D., Marin-Perez, R., and Skarmeta, A. (2020). Secure authentication and credential establishment in narrowband iot and 5g. *Sensors*, 20:882.

Sanchez-Iborra, R., Sánchez-Gómez, J., Pérez, S., Fernández, P. J., Santa, J., Hernández-Ramos, J. L., and Skarmeta, A. F. (2018). Enhancing lorawan security through a lightweight and authenticated key management approach. *Sensors*, 18(6):1833.

Schrecker, S., Soroush, H., Molina, J., Hirsch, J. L. F., Buchheit, M., Ginter, A., Martin, R., Banavara, H., Eswarahally, S., Raman, K., King, A., Zhang, Q., MacKay, P., and Witten, B. (2016). Industrial internet consortium (iic) - the industrial internet of things volume g4: Security framework.

Xing, J., Hou, L., Zhang, K., and Zheng, K. (2019). An improved secure key management scheme for lora system. In *2019 IEEE 19th International Conference on Communication Technology (ICCT)*, pages 296–301.

Yu, C.-E., Wang, C., and Zhang, S.-Q. (2022). Fault-tolerant energy-efficient lorawan networking architecture. In *2022 11th Mediterranean Conference on Embedded Computing (MECO)*, pages 1–4. IEEE.