Security Aspects in an Intelligent Lighting System for Public Squares using Fog Computing

Wesley R. Bezerra[1], **Cristiano A. Souza**[1], **Carla M. Westphall**[1], **Carlos B. Westphall**[1]

[1]LRG – Universidade Federal de Santa Catarina (UFSC)
Florianópolis – SC – Brazil

{wesleybez,cristianoantonio.souza10,carlosbwestphall}@gmail.com,
carla.merkle.westphall@ufsc.br

Abstract. *Security in public spaces is a fundamental factor for citizens and can be provided by digital tools such as remote sensing. However, the security of such tools is also an important issue, and violating this security can lead to the susceptibility of loss of security in public spaces. This work presents a use case where an authentication solution is applied to ensure security in a smart lighting system in public squares. The use case, the adversary and its motivation, the threat modeling of the system, and a general discussion about this study are presented. As a result, a threat model with countermeasures is presented, and security aspects brought about by the use of the adopted multi-factor authentication mechanism with reputation are discussed.*

1. Introduction

Security in Internet of Things (IoT) devices has been a concern and research subject over the last few years [Deep et al. 2019]. According to some authors [Yi et al. 2015, **?**, **?**], the number of available devices tends to grow exponentially, which brings some complexities to using these devices to access services, especially services to citizens. These difficulties are related to aspects of transmission technology and security aspects of the use of such systems.

In smart cities, one of these concerns is citizen security and how this can be affected if a city service suffers a security breach because it is not correctly implemented or well configured for its best use [Miessler 2015, Tiburski et al. 2019]. An example is the flood measurement service in Rio do Sul - SC[1], which presents real-time information on the river level through a web panel, and this information is used to make decisions about whether or not to evacuate their homes. If such a service becomes unavailable, the population may have access to less information and thus hinder decision-making at the right time.

Therefore, security for citizen services in smart cities is highly relevant and not optional. Even if some parts of the system, such as sensors, do not have the computing power to guarantee a level of security using encryption or very robust transmission protocols, a security guarantee is necessary for this type of service.

Some related works, even briefly, on smart lighting are worth mentioning. In the work of Biundini et al. [Biundini et al. 2024], a solution is presented that uses LoRaCELL, a solution that adopts LoRaWAN in transmitting data from a set of sensors.

[1]https://defesacivil.riodosul.sc.gov.br/index.php?r=site\%2Findex

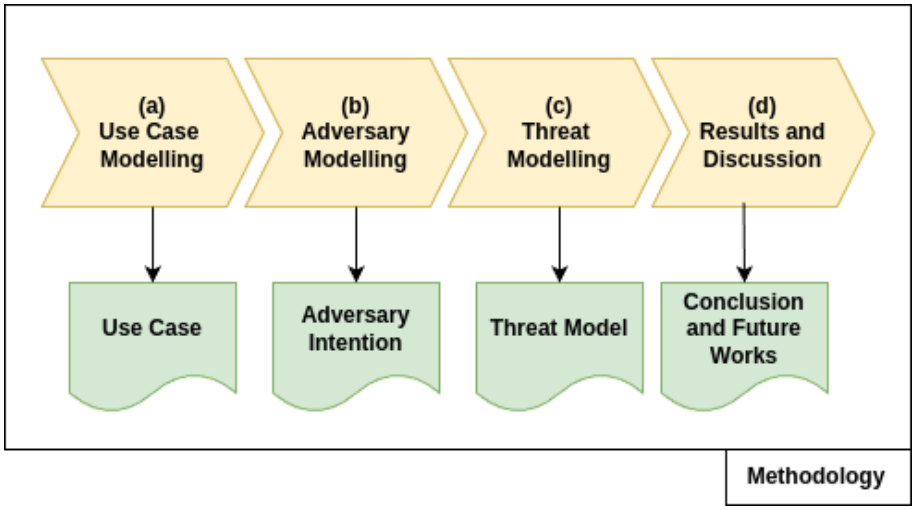

Figure 1. Methodology

Also, we have the work of Srinivasan et al. [Srinivasan et al. 2024] that applies this concept of smart lighting to agriculture. Finally, Marsi et al. [Masri et al. 2024] present the design of a physical smart pole using ESP and discuss aspects such as energy consumption and other metrics. As a result, although a limited number of works, we can note that this is an area of significant importance for Smart Cities and sustainability in public lighting.

In this work, we will use a fictitious case of Smartlight for a public environment: a square. The square is a public environment where citizens can walk, take their families, socialize with neighbors and other residents of the region, and, in other words, have moments of leisure in the community. However, this environment can be targeted by people of bad character who want to commit crimes (i.e., using drugs in public places, encouraging drug use, or even selling illicit substances).

The paper is organized as follows: section 2 presents the methodology used to develop this paper. Following, section 3 presents the development of this paper in four phases: subsection 3.1 presents the use case, subsection 3.2 presents an adversary modeling, and subsection 3.4.1 presents the threat modeling. The section ends with a discussion of the results in subsection 3.4. Finally, section 4 presents the conclusion and the set of proposed future works.

2. Methodology

This work occurs in four stages with four results (Figure 1). Each stage has its specific result. All stages were developed using the Open Science concept [Hosseini et al. 2025, Mirowski 2018, Pordes et al. 2007] and are described in a repository in the Open Science Framework (OSF) [Foster and Deardorff 2017, Von Bertalanffy 1968]. To access any file related to the development of this work, follow the link[2].

In the first stage (a), the parts that make up the smart public light system are described. The relationship between the parts of the system is established, as well as how the sensor is composed in terms of its subsystems. The limitations of the type of

[2]https://osf.io/eb329/?view_only=0f38930a22764bfab1ed6f41b62a9dfa

network protocol used and the type of restricted device used are specified. In addition, it is discussed how the use of MFA_R [Bezerra et al. 2023a, Bezerra et al. 2023b] impacts the system's security.

Moving on to the second stage (b), the adversary is modeled. Aspects of its intentions to violate the system and benefits related to these violations are brought up. Some of its capabilities as an agent on the intelligent lighting system are also listed. Consequently, a general modeling of an adversary is obtained to analyze possible threats to be modeled.

Next, the threat modeling of the system (c) and the description of the attack surfaces are carried out. In this stage of the work, general threats to the system, the components, and communication are modeled, and specific threats to the components are classified and prioritized, concluding with the proposal of countermeasures. This is the main contribution of the analysis of this work.

Finally, the results are commented on, and improvements are proposed for future iterations. Security aspects that were resolved by MFA_R are discussed and compared to other forms of resolution. Security aspects of the service and for citizens are followed by other complementary analyses that can take place in this system for its continued improvement.

3. Development

3.1. Public Square Lighting Use Case

To better understand the security problems in the TM, a use case of smart lighting service for municipal squares is proposed here. This service aims to save energy through the Internet of Things for monitoring and acting in the regulation of the lighting intensity of the squares of a given city C. As a public lighting service monitored with IoT, it is classified in the *Smart Cities* area of activity.

The service proposes to solve the following problem. At night, the city squares automatically light up with their maximum luminosity, wasting energy when it starts at dusk and dawn when it is not yet completely dark. Still, as a problem, it can be highlighted that even without citizens walking in the squares, lighting continues at its maximum potential, consuming energy unnecessarily. A smart lighting service was proposed (hypothetically) to save energy in the city C.

During the dawn and dusk periods, brightness sensors that detect the assessment of sunlight are used to calibrate the brightness intensity required for the square (P). This way, during the transitions of the sun's luminosity, the city saves energy by C. Another feature is the detection of passersby. When no people are walking around the square P, the intensity of the square's lighting drops by 50%, causing significant energy savings.

As for the network architecture the service uses, its data is transmitted using LPWAN. The decision-making on the intensity of the square's lighting is made in a Fog Node (part of the Fog Computing architecture). If there is network unavailability for a certain period, the service will be *bypassed*, and the lighting will work at its maximum during this period.

The IoT device consists of four main elements (Figure 2): the LPWAN network device, restricted hardware (i.e., esp32), the lighting actuator, and a photoelectric sensor.

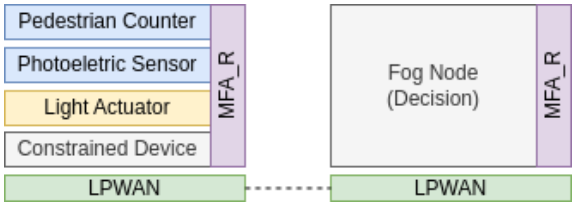

Figure 2. Description of the architecture used in the smart lighting service - on the left is the sensor with its four layers (network, processing, actuator and sensor - from bottom to top) and on the right is the Fog Node with its two main layers (network and service).

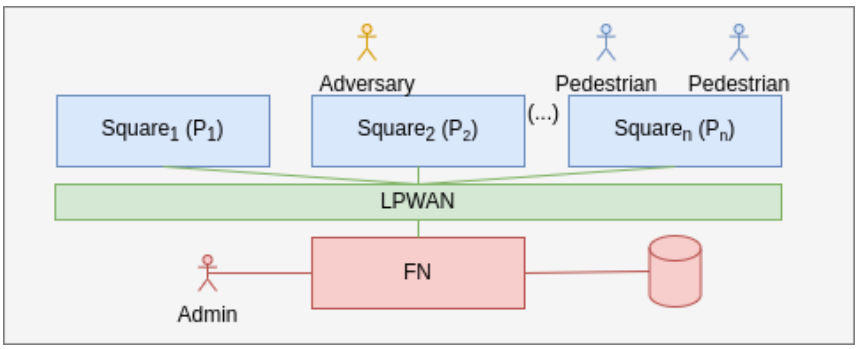

Figure 3. Overview of modeling the smart lighting use case. Square $P1$ has no passers-by, Square $P2$ has an opponent, and Square Pn has two passers-by. All communicate via LPWAN with the Fog Node (FN).

The LPWAN network device provides low power, long-distance *link* at a low cost to implement the service. On the other hand, the restricted hardware allows the implementation of the project at a reduced cost for citizens. The lighting actuator allows the configuration of the required lighting intensity according to the evaluation of the Fog Node. Finally, the photoelectric sensor captures the amount of sunlight falling on the square and regulates intensity for better use of natural light.

However, a security breach in this system can favor different adversaries. This work will describe the illicit drug dealer (adv_{d}). This adversary's goal is to sell his product in an environment with low lighting, making it more difficult for the police to identify it. For this adversary, it is important to circumvent the system without interrupting its operation because the lighting will adopt maximum intensity once the system is interrupted. In this way, it is important for the adversary that the Fog Node receives wrong measurements of the amount of incident sunlight and the number of passersby. If this happens, the opponent can achieve financial gain and remain unaccountable.

This work, MFA_R is used as an authentication solution that can respond adequately to the adversary's attacks. Since it is multi-factor authentication, MFA_R makes the types of threats associated with this type of adversary more difficult. Also, through reputation score and built-in security features, this authentication mechanism can, in a lightweight manner (without using cryptography), provide a robust solution to security problems in authentication for Smart Cities. This way, the proposed lighting scenario will exemplify the threat modeling workflow for complex distributed security mechanisms. Finally, it will be possible to validate whether the workflow meets the threat modeling

needs for this type of mechanism in potential Smart Cities scenarios.

Through this use case, the threats listed in the work will be analyzed, and the countermeasures implemented in MFA_R to avoid them will be discussed. Using scenarios makes it easier to understand how countermeasures work, the costs of carrying out a threat, and the limitations found in the LWPAN and Constrained Devices scenario in the area of *Smart Cities*.

For comparative purposes, each lighting item ($pole$) must be considered as a device that must be authenticated; the gateway that will provide the authentication will be in a building of the power utility, communication is done through an LPWAN link, and only the adversary modeled in this section will attempt to breach system security. Through these premises, it is possible to analyze the desired aspects of security and authentication for this fictitious use case.

Some definitions are important at this point for a better **formalization of the use case**. In this section, we will define the parts of the use case, such as the fog node, square, sensors, subjects, adversary, and the system as a whole.

$$FN_i = \{decision\_mechanism, MFA\_R, lpwan\_link\} \tag{1}$$

Starting with the **fog node** (1), it consists of three parts: the decision engine, the MFA_R, and the LPWAN link. The decision engine is the software part that analyzes the system behavior and decides when to turn on/off the lights on the street lamps. The MFA_R is the component responsible for service-side authentication and ensures the identification of the sensors in the system. Finally, using a low-cost link, the LPWAN link is responsible for data transmission.

$$\begin{aligned} sensor_i = \{&pedestrian\_counter, phoeletric\_sensor, \\ &light\_actuator, constrained\_device, MFA\_R, lpwan\_link\} \end{aligned} \tag{2}$$

In turn, the **sensor** (2) is composed of six parts. The pedestrian counter checks how many pedestrians pass near the pole and starts a timer when no more pedestrians pass. The photoelectric sensor captures the amount of light that the region where the pole is receiving. The $light\_actuator$ interacts by turning the power of the lighting pole on/off according to the decision made in the fog node. The MFA_R is responsible for authenticating the sensor in the system and performing authentication enforcement processes, if necessary. Finally, the $link\_lpwan$ connects the sensors to the service running on the fog node (FN_i).

$$pole_i = light_i, sensor_i \tag{3}$$

The **pole** (3) is defined by the pair of lighting and sensor. Lighting is the fundamental element of the pole and allows it to illuminate the area around it. The sensor is the component that, associated with the lighting, will make the pole intelligent and thus provide a more economical and appropriate service to the citizen.

$$Pedestrians = \sum_{j=1}^{\text{n}} pedestrian_i \tag{4}$$

$$adv_i = malicious(pedestrian) \tag{5}$$

Pedestrians (4) can be defined as people passing through a square at a given time. Even though the system does not directly control pedestrians, their presence is a fundamental part of the decision-making process in the square's lighting process. No less important is the definition of the adversary (adv_i), which is defined as a malicious pedestrian (5).

$$square_i = Pedestrians, Poles \tag{6}$$

$$city_i = \sum_{j=1}^{\text{total}} square_i \tag{7}$$

$$region = \sum_{j=1}^{\text{total}} city_i \tag{8}$$

As for the definition of places, we have the definition of $square$ (6), $city$ (7), and $region$ (8). A $square$ is defined as a set of posts and pedestrians. A $city$ is defined in our system as a delimited set of squares. A $region$, in turn, is a set of cities.

$$system = \{region, FN\} \tag{9}$$

As a final definition, the system is understood as the fog node and region pair. In other words, each system must be responsible for a region and have a fog node for this given region. Thus, one of the consequences of this definition is that an adversary from a specific square in a specific city can access and threaten the system of an entire region. Another consequence is that once the adversary is identified, he will be removed from the system that serves all the cities in the region.

3.2. Adversary Model

This adversary was designed with the desire to breach the system in order to become immune and invisible to cameras or police officers. This way, he could not be identified from afar by authorities and could escape and blend in with other people. So, his primary purpose is to circumvent the system so that it turns off and reduces the amount of light emitted so that it can go unnoticed.

It can be assumed that the adversary has advanced networking knowledge or can hire someone with this knowledge to breach the system. He follows the Dolev-Yao precepts [Dolev and Yao 1983]. In this way, he can try to breach the device's security in the transmission or even try to access the system on the fog node.

Table 1. List of use case symbols

Symbol	Mean
$light_i$	public lighting system
$pedestrian_i$	a person walking in the square
C_i	City
P_i	Square
adv_{d}	adversary
$Pedestrian$	set of pedestrians
$square_i$	*ith* square
$pole_i$	*ith* pole
$Poles$	set of poles
$sensor_i$	*ith* sensor

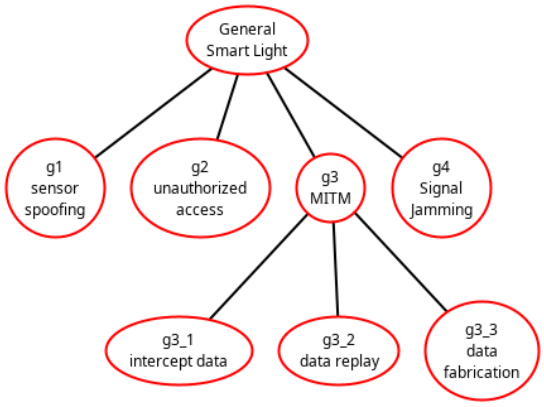

Figure 4. General Attack Tree

3.3. Threat Modelling

This subsection will present the artifacts brought by the threat modeling performed. The following will be presented:

1 General Attack Tree;
2 Data Flow Diagram;
3 Components Attack Tree;
4 Classification and Prioritization;
5 Countermeasueres.

The General Attack Tree brings to light general system problems and does not consider specific component details. This type of analysis looks at the system as a black box and is the first approach in system security analysis. As shown in Figure 4, problems such as unauthorized access, spoofing, man-in-the-middle (MTIM), and jamming can generally affect the system.

As for the DFD (**2**), which presents the system components and how they communicate, this is an important step to understand better the dynamics of communication between the exchanged parts and how this can affect the system's security as a whole, it is also at this stage that the internal components of the system are exposed, if necessary.

As we can see in Figure 5, the sensor exchanges information with the Fog Node in three moments. The Fog Node saves the data locally, so there are no problems with remote access to the Fog Node data repository.

The first message ($mfar\_auth$) encapsulates the sensor authentication process on the fog node using MFA_R. This process occurs in three stages and continues by monitoring the published data to guarantee continuous security for the system and the authenticated sensor. The following message is the $illumination\_data$, which carries the lighting sensor data and the $auth\_code$ generated in the MFA_R authentication process. The last message is sent from the fog node to the sensor, which sends the configuration data so the system can adequately illuminate the square.

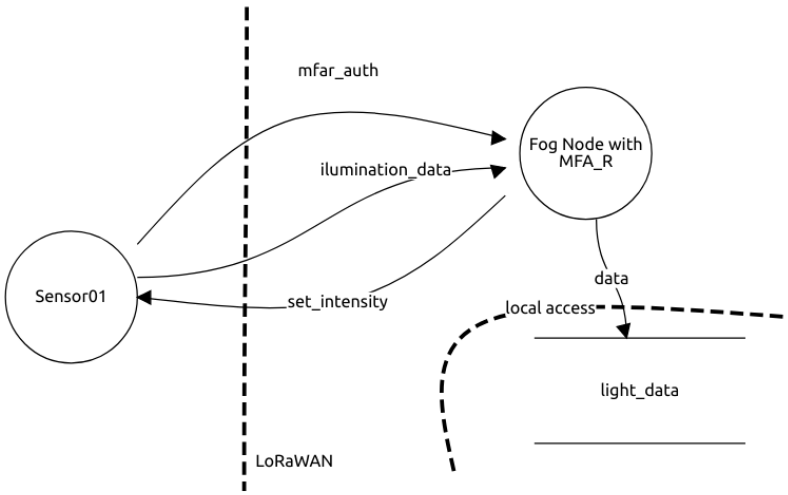

Figure 5. Data Flow Diagram

Next, we have threat modeling in the components. In this scenario, we will analyze the Sensor and Fog Node threats. As we can see in Figure 6, The threats to the fog node component are specific, as in the case of **Data Violation**, which is a specific violation of this component and is not transparent to users who do not know the system architecture. In this way, threat modeling, considering internal aspects of the system (gray box), provides important information for decision-making during threat mitigation, even if these are implicit.

STRIDE and CVSS were used for classification and prioritization, respectively. With STRIDE, we can classify threats according to their acronyms: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. With CSVV, threats are prioritized with a value from 1 to 5 (where 1 is the least priority and 5 is the most priority).

The table 2 presents us with an overview of all the threats in our use case, separated by Attack Surface. Three attack surfaces are presented: the general, the sensor, and the fog node. Some threats that appear in general are not repeated in the components. However, we will only comment on them once. In general, spoofing and impersonation of the fog node can cause problems for the entire system by injecting false data and leading to incorrect lighting configuration. Another important problem is improper access to the system, which can cause damage to the system's continuity if someone violates the

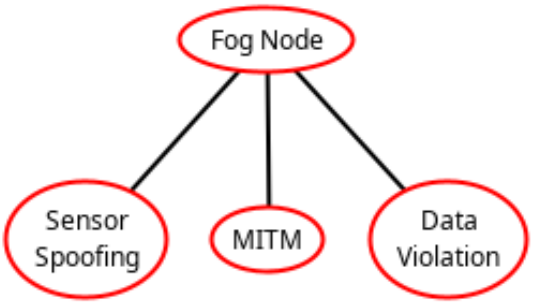

Figure 6. AD Sensor

Attack Surface	Threat	Classification	Prioritization
General	Sensor Spoofing	S	5
	Unauthorized Access	E	5
	MITM	T I	3
	Jamming	D	1
Sensor	Fog Node Impersonation	S	3
	MITM	T I	3
	Jamming	D	1
Fog Node	Sensor Spoofing	S	5
	MITM	T I	3
	Data Violation	I E	3

Table 2. Threats classification and priorization

security of the fog node. MITM attacks can occur in various parts of the system and are mainly related to data transmission and access to transmitted data. Finally, jamming attacks are less of a priority.

In a real implementation case, this table would be more extensive and should consider details of the chosen technologies and programming languages, platforms, operating systems, etc.; However, these details will be abstracted in our fictitious use case.

Attack Surface	Threat	Countermeasure
General	Sensor Spoofing	MFA_R authentication
	Unauthorized Access	MFA_R authentication
	MITM	LoRaWAN characteristics and MFA_R authentication
Sensor	Fog Node Impersonation	MFA_R authentication
	Data Violation	Firewall and DB configuration

Table 3. Countermeasures

In its last stage, a set of countermeasures to mitigate the threats raised is expressed in Table 3 and Figure 7. The countermeasures are presented visually in the figure and in

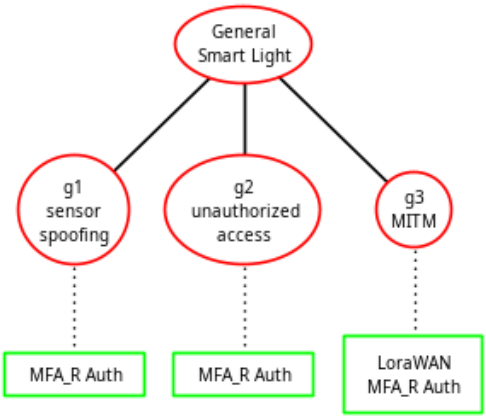

Figure 7. Countermeasueres

greater detail in the above table. Regarding the countermeasures used, we can see that MFA_R already meets the security needs of the system. This type of solution is provided by the way this mechanism works. It provides two-factor authentication and a third factor that provides continuity through evaluating the published data. In this way, we can guarantee that it is impossible to use the system without two levels of authentication [Bezerra et al. 2023b] and that the data will be continuously evaluated. If there are nonconformities in the system's operation, the enforcement process will ensure that the sensor has to authenticate again or exit the system.

In summary, a multi-factor authentication mechanism with reputation is an adequate solution for security in Smart City systems that use restricted devices and low-power networks for data transmission. In addition to not consuming much battery for data transmission and not requiring large processing and memory capacities to execute its authentication processes, this solution is secure and linked to protocols such as LoRAWAN, which can guarantee security at various stages of the system's operation.

3.4. Results and Discussion

This section discusses the impact of threats found throughout the process in the use case presented in Section 3.1. Furthermore, solutions and **Countermeasures** for possible **System Violation** are discussed, considering threats from an overview (black box analysis) and specific threats for each of the components of the mechanism (grey box analysis).

In short, this part of the work presented the CMs and how they were materialized in the project. Although not all of them have become implementations of security devices, the recommendations and assumptions listed also serve as mitigations. It follows with the exposition of the relationships between threats and countermeasures to allow the visualization of how mitigations happen in practice.

3.4.1. Threats and Use Case Analysis

A correction was made between the threats and their consequences for the security of this system. In addition, general and component-specific threats were analyzed—previously expressed through the outlined ADTs. Now, see below the practical consequences of not implementing countermeasures in this scenario.

Starting with unauthorized access to the lighting system. This threat would allow the opponent to dim or even turn off the lights remotely. Thus, with the remote control of the lighting in the public square, the adversary could commit incognito crimes without being held accountable by law. As shown in Table 2 with CVSS, this is a significant threat to the model and has high priority.

To spoof the sensor, the opponent could control the luminosity of a specific pole. That way, he would create a safe place and commit crimes without being easily noticed by passersby or patrolling police.

Also, as a man-in-the-middle, the adversary could capture, replay, and fabricate data when trying to breach the system's security. Such an attack would require an opponent with greater computational skills, which is less likely – but not impossible. However, some problems related to data transmission integrity in LPWAN are well resolved, such as the LoRAWAN protocol that addresses this issue.

Data violation attacks were not covered in detail. This type of attack is quickly resolved by configuring database access. For instance, some banks may restrict which IPs can access each database or even restrict it to only a particular network segment. Another option is to reinforce this security with an appropriate firewall configuration.

Thus, the use case showed the challenges of implementing a public service. Many of the security challenges are related to implementing the service without an adequate authentication mechanism and the restrictions imposed on the CD and LPWAN environment. As a result, it can be said that even with this scenario's current challenges, security and authentication in public services are essential factors.

3.4.2. Result Analysis

With a smart environment prepared for this situation, a delinquent citizen may feel threatened and try to violate the system's security to avoid being punished by law. Our use case involves an intelligent system of pole lamps for lighting public squares. This system aims to save money and only turn on the lighting when the sensor integrated into a Fog Node processes the information on adequate lighting for the presence of passersby and how to act on the lighting.

Likewise, deciding when to turn off this lamp is crucial in providing the service. The idea is that the city can save money by not always leaving the lamp on with its maximum lighting potential (lighting intensity) when necessary. In this way, when there are no passersby, the system can reduce the lamp's light intensity in the monitored area.

This directly affects our adversary in question since if he can sell drugs, for example, the environment should be poorly lit and not easily seen from afar. As a result, the

drug dealer would be exposed to the light since the system would identify his presence and activate more excellent light.

4. Conclusion and Future Work

This work successfully presented the use case of smart lights for public squares in Smart Cities using a multi-factor authentication mechanism with reputation. During the work, we were able to understand which parts make up this type of system, what the intentions of the adversary modeled in this case are, the threats that this adversary can execute, and, mainly, how they can be eliminated using adequate authentication.

Together with other works that expose MFA_R through experimentation such as [Bezerra et al. 2023b, Bezerra et al. 2023a] or that provide an analysis of security aspects of message protocols [dos Reis Bezerra and Westphall 2020], it can provide better clarification on how the mentioned mechanism works.

In future work, it would be important to perform a simulation using a network tool such as Omninet++ or ns3 to evaluate the network performance of the proposed use case. Another aspect of possible evaluation is the possibility of analyzing the energy consumption of the devices involved and deciding on the best configuration. No less important is a qualitative analysis of the data, which involves collecting metrics in a simulated environment, or preferably a real one, to refine the analysis. Finally, it would also be important to formally verify the security protocol in conjunction with the LoRAWAN security protocol in a tool such as ProVerif. This would guarantee the security aspects of the protocol in conjunction with MFA_R.

5. Acknowledgments

The authors sincerely thank the Federal University of Santa Catarina (UFSC). This study was partially funded by the Fundação de Amparo à Pesquisa e Inovação do Estado de Santa Catarina (FAPESC), Edital 20/2024.

References

Bezerra, W. D. R., Boing, R. D. N., de Souza, C. A., and Westphall, C. B. (2023a). An experimentation on coap multi factor authentication mechanism with reputation for internet of things constrained devices and low power wide area network. In *2023 International Conference on Information Networking (ICOIN)*, pages 67–72. IEEE.

Bezerra, W. R., Martina, J. E., and Westphall, C. B. (2023b). A formal verification of a reputation multi-factor authentication mechanism for constrained devices and low-power wide-area network using temporal logic. *Sensors*, 23(15):6933.

Biundini, I. Z., Pinto, M. F., Honório, L. M., Capretz, M. A., Timotheo, A. O., Dantas, M. A., and Villela, P. C. (2024). Loracell-driven iot smart lighting systems: Sustainability in urban infrastructure. *Sensors*, 24(2):574.

Deep, S., Zheng, X., and Hamey, L. (2019). A survey of security and privacy issues in the internet of things from the layered context. *arXiv preprint arXiv:1903.00846*.

Dolev, D. and Yao, A. (1983). On the security of public key protocols. *IEEE Transactions on information theory*, 29(2):198–208.

dos Reis Bezerra, W. and Westphall, C. B. (2020). Avaliação de desempenho de protocolos de mensagens com arquitetura publish/subscribe no ambiente de computação em nevoeiro: um estudo sobre desempenho do mqtt, amqp e stomp. In *Anais do Workshop de Pesquisa Experimental da Internet do Futuro*, pages 7–12. SBC.

Foster, E. D. and Deardorff, A. (2017). Open science framework (osf). *Journal of the Medical Library Association: JMLA*, 105(2):203.

Hosseini, M., Horbach, S. P., Holmes, K., and Ross-Hellauer, T. (2025). Open science at the generative ai turn: An exploratory analysis of challenges and opportunities. *Quantitative Science Studies*, 6:22–45.

Masri, M., Liestyowati, D., Andiyan, A., and Husolihah, A. (2024). Smart energy public street lighting system. In *IOP Conference Series: Earth and Environmental Science*, volume 1301, page 012008. IOP Publishing.

Miessler, D. (2015). Securing the internet of things: Mapping attack surface areas using the owasp iot top 10. In *RSA Conference*.

Mirowski, P. (2018). The future (s) of open science. *Social studies of science*, 48(2):171–203.

Pordes, R., Petravick, D., Kramer, B., Olson, D., Livny, M., Roy, A., Avery, P., Blackburn, K., Wenaus, T., Wurthwein, F., et al. (2007). The open science grid. In *Journal of Physics: Conference Series*, volume 78.

Srinivasan, S., Shoba, L., Alavanthar, T., Srinivasan, C., Murugan, S., and Sujatha, S. (2024). Iot-enabled horticultural lighting for optimizing plant growth and agriculture operations. In *2024 2nd International Conference on Networking and Communications (ICNWC)*, pages 1–7. IEEE.

Tiburski, R. T., Moratelli, C. R., Johann, S. F., Neves, M. V., de Matos, E., Amaral, L. A., and Hessel, F. (2019). Lightweight security architecture based on embedded virtualization and trust mechanisms for iot edge devices. *IEEE Communications Magazine*, 57(2):67–73.

Von Bertalanffy, L. (1968). General system theory. *New York*, 41973(1968):40.

Yi, S., Hao, Z., Qin, Z., and Li, Q. (2015). Fog computing: Platform and applications. In *2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*, pages 73–78. IEEE.