An HTTPS-based authentication and authorization method for low-cost IoT devices in smart water metering

Felipe C. Leal
Universidade Federal de Sergipe
Sao Cristovao, Brazil
felipecarvalho5520@gmail.com

Marcos V. S. Melo
Instituto Federal de Sergipe
Lagarto, Brazil
marcosvinicius.sm@icloud.com

Alfredo M. Vieira
Instituto Federal de Sergipe
Lagarto, Brazil
alfredo.vieira@ifs.edu.br

Rubens de S. Matos Junior
Instituto Federal de Sergipe
Lagarto, Brazil
rubens.junior@ifs.edu.br

***Abstract*—IoT technologies have been enabling real-time monitoring of resources, such as water and electricity consumption, and therefore leveraging the development of smart buildings. Preventing resource wastage is a major concern in the management of household, commercial, and industry environments. Decision-making on such a context depends on how reliable are the sources of incoming data. The enforcement of security aspects in such systems is challenging because of the decentralized, distributed, and resource-constrained devices. This paper presents an authentication and authorization approach for low-cost IoT devices, that is based on HTTP and SSL protocols (known as HTTPS). The proposed solution includes a lightweight API that addresses the approval of motes and sends security tokens, so we assure that only legitimate and authorized devices are registered in the system and guarantee that every incoming data come from those authorized devices. This approach is tested at the context of the SPARC project's smart water metering infrastructure.**

***Palavras-chave*—Internet of Things; security; smart cities**

I. Introduction

In 2015, the United Nations General Assembly (UNGA) set the "2030 Agenda", which is a set of goals to guide the world toward a path of sustainable development, focusing on socioeconomic and environmental dimensions [1]. In this context, sustainability is the balance between meeting human needs and preserving natural resources, utilizing them without compromising the ability of future generations to meet their own needs. Potable water is one of the natural resources that deserves most attention and care for its preservation [2].

However, it is estimated that by 2025, over half of the world's population will suffer from water scarcity in their homes. Research conducted in 2022 by the World Health Organization (WHO), the United Nations Children's Fund (UNICEF), and the World Bank concluded that 25% of the population still lacks access to clean water [3], and at least 1.42 billion people – including 450 million children – live in areas of high or extremely high water vulnerability [4]. The climate changes, escalating each year, exacerbate the intensity of droughts and floods, leading to water insecurity, disrupting water supply, and devastating communities [5]. Meanwhile, rapid urbanization further strains cities' capacity to provide water for millions living in informal settlements and slums.

Taking into consideration human interaction with nature, several laws aimed at protecting water resources have been developed. In 1981, U.S. Law No. 6,938/81 was enacted, which deals with the National Environmental Policy - PNMA and establishes in its article 4 that it shall aim: "[...] VI - at the preservation and restoration of environmental resources with a view to their rational use and permanent availability, contributing to the maintenance of an ecological balance conducive to life [6]. The United Nations formally recognized that clean drinking water and sanitation are essential for human dignity and well-being [7].

In environments such as buildings, one can observe that structural problems are the main causes of water wastage, invisible leaks, structural issues in masonry boxes, or misuse of water. There is a high rate of wastage also in houses in peripheral areas, due to the precariousness of the installations. Brazil is privileged in terms of hydric availibility, However, currently, the total water withdrawal in Brazil is estimated at 64.18 trillion liters per year, divided as follows: irrigation (50.5%), urban supply (23.9%), and industry (9.4%). Other uses considered were animal use (8%), thermoelectric plants (5%), rural supply (1.6%), and mining (1.6%) [8].

Internet of Things (IoT) technologies have been enabling real-time monitoring of resources, such as water and electricity consumption, and therefore leveraging the development of smart buildings. The IoT concept refers to interconnected devices that collect, analyze, and exchange information in real

time, wherein sensors and actuators blend seamlessly with the environment around us [9], [10]. Linking the use of IoT to the pillars of sustainability and resource management plays an important role in building an ecologically sound future. Preventing resource wastage is a major concern in the management of household, commercial and industry environments. Decision-making on such a context depends on how reliable are the sources of incoming data.

The enforcement of security aspects in such systems is challenging because of the decentralized, distributed, and resource-constrained devices. It is a challenge to protect IoT systems from attacks that usually aim at building botnets or other dangerous purposes. If an attacker takes control of a metering device, it can send false data to the servers and try to gain access to the server by injecting malicious code or benefit from failures in data collection protocol.

This article aims to present the design, prototyping and implementation of a secure and cost-effective option that can be implemented in smart buildings for industry, commerce and residential environments. The proposed solution comprises a set of devices, embedded software and security mechanisms, integrated along with an API and dashboard to process, store and display relevant information about water consumption but that is also able to host other monitored data about electricity consumption and gas concentration.

II. Related Works

The rise of new sustainable development measures and the growing efforts to find effective natural resource management solutions, many emerging technologies have been proposed. Some of them promote the interconnection of all things to achieve efficient monitoring and control of resources, such as [11]. The 'smart management' of resources through IoT enables the assurance of adequate water supply and contributes to the use of technology for the prediction of possible extreme events, efficient utilization of these resources, and practical management in supply systems [12].

A recent project carried out by researchers from the Federal University of Ouro Preto (UFOP) in 2021 [13] proposed an intelligent system aimed at measuring water consumption and consequently detecting leaks in the hydraulic network based on the collected data. Additionally, the presence of wireless protocols could also be observed, as this tool in residential environments, and especially in schools, can mitigate and provide accurate resolution of leaks and consumption analysis.

The work presented in [14] describes a project at Eurípides University Center of Marília, using Arduino and flow sensors for the proper water rationing, discussing the potential use of IoT in water resource management. In the context of water supply problems in various regions of Brazil, a solution for monitoring residential water consumption was presented, consisting of measuring modules at the consumption points of the residence. A web application receives information from the sensors and makes it available to the end-user in the form of consumption graphs for the specific points in the residence.

In the University of Campinas, a smart campus project produced an IoT application for smart monitoring of water distribution [15]. Their work had the goals of detecting leaks and predicting water consumption, being part of a set of other IoT-enabled technologies for enhancing academic community daily routine.

In the work presented in [16], a solution is presented for controlling and monitoring energy consumption and automating academic services, such as student attendance through facial recognition. The FIWARE middleware was integrated into the solution architecture to handle heterogeneous communication, storage, and processing of context data.

The authors in [17] discuss how traditional network security cannot be directly used in IoT networks due to its limitations on computational capabilities and storage capacities. In their paper, they have focused on surveying IoT security, particularly on their authentication mechanisms. The authors highlighted enormous attacks and technical methods on the IoT authentication mechanism. Additionally, they discussed existing security verification techniques and evaluation schemes of IoT authentication.

In [18], the authors propose an efficient secured group-based lightweight authentication scheme for IoT based E-health applications; their scheme authenticates and establishes secure channels through sensor nodes and base station. The proposed method with a feature of the group-based node reduces distance and consumed energy, as well as leads to reduced communication cost.

III. Smart water metering device

The proposed IoT-based water metering solution was designed in the scope of the SPARC (Smart Prediction and Analysis of Resources in a Connected Campus) project. It employs water flow sensors, that measure the flow of liquid through piping, allowing us to use this data to analyze the usage of water resources.

The union of these sensors with IoT technology is an fundamental element to make it possible to use it in large scale. Processing such data enables to prevent water leaking, predict consumption and charges and apply active management, e.g., by deploying devices that are able to block the water flow. A large variety of flow sensors available can be integrated in this approach, empowering data collection from many sources of the same building and thus enabling better predictions of any type of water wastage.

The device case is made with a custom 3D printed model. The use of the 3D printing technology allows us to quickly prototype, develop, test and adapt the device to any situation in addition to facilitate the device production and replication. The device case requires 39.24g of filament to be printed. As shown in Figure 1, it uses the following components: 3D printed case, ESP8266 NodeMCU microcontroller, P4 connector, power switch, and a 0.96 inches monochrome oled display. The flow sensor is attached externally. Some types of sensors can be attached, requiring only little code adaptions to work properly. The sensor employed in the current prototype is the YF-S201, measuring the flow range between 1-30 L/min.

The final size of the SPARC mote prototype is 5 cm x 7 cm x 4.5 cm (without the flow sensor), which is a small size that allows us to fit the device in almost any location. In this way, it is possible to deploy devices throughout every building, collecting and analyzing data for the most diverse management purposes.

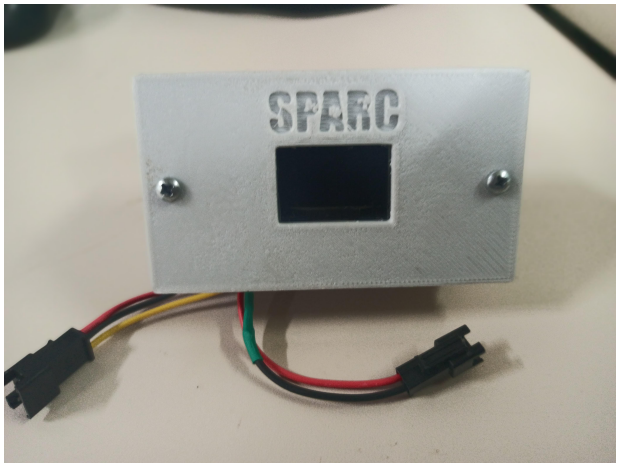

Fig. 1. Assembled SPARC Mote Device

The choice of ESP8266 NodeMCU as the processing component for SPARC is mainly due to being an inexpensive microcontroller with WI-FI integration and the required digital pins for connection of remaining components. The data connections are made using D1, D2 and D7 pins, where the D1 and D2 pins refers to SLC (signal clock) and SDA (signal data) of the oled screen and D7 is connected to the flow sensor data pin. The power comes from a P4 power input, which connects to the ground pin (directly) and the Vin pin (through a power switch), as shown in Figure 2. The SPARC mote device enables real-time sectorized water metering, by deploying a single mote in each point of water usage, each floor/building of a campus/company, being each device independent from the others, but connecting via Wi-Fi network to the server (made with [19]) which hosts the API for device authentication and the dashboard for data visualization. This solution design enables to distribute the devices efficiently, ensuring that all necessary areas are being monitored.

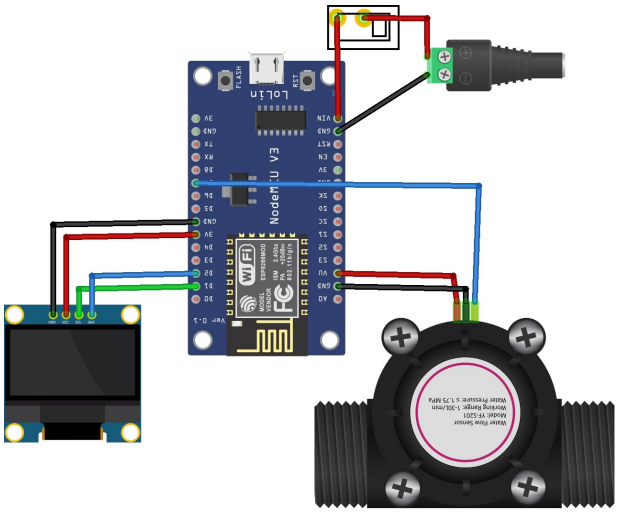

Fig. 2. SPARC Mote Assembly Schema

IV. Authentication and Authorization Method

The data transmission happens using HTTP and TLS protocols (HTTPS), however, before allowing data transmission from a mote device to the server, a custom authentication and authorization protocol must be used, as seen in Figure 3. The authentication depends on the device's MAC (medium access control) address, which is unique, and an API token which is modified every time the device authenticates. The API token is based on uuid4, an universal identifier based on RFC 4122 standard [20].

In order to start the authentication process and register a device, the device must first send its own MAC and IP addresses to the server, which will create a pending approval process that needs to by authorized by the system administrator. After approved, the device will need to make another request to get the token to authenticate when sending data to the server. If the device is not approved by the system administrator but tries to send data anyway, the data will not be processed, but the request will be stored in the logs containing the device's MAC address, IP, ID and request time.

Once the device is authorized, effective data transmission may begin. Using HTTPS, through the POST method, the device sends its token and the data collected in the last 5 minutes. It is worth highlighting that both token and sensor data are encrypted due to the TLS protocol, so the system is

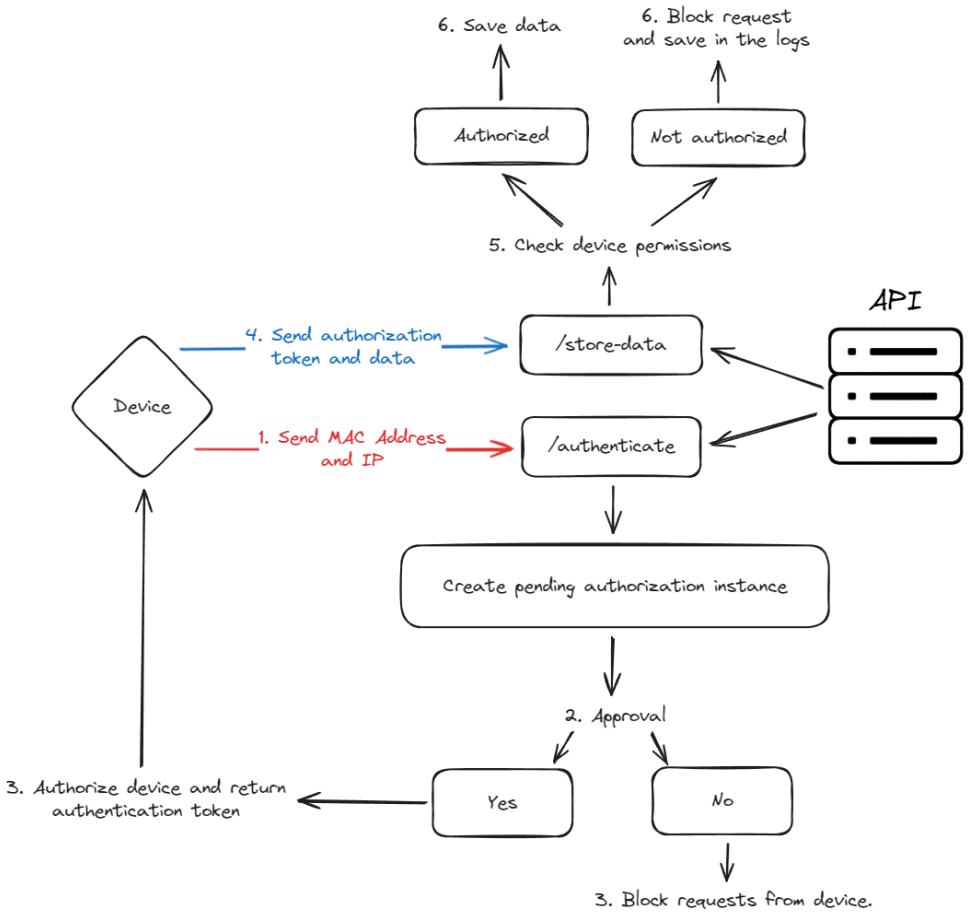

Fig. 3. Authentication Protocol

protected against evesdropping and intruders attempting to send data reusing a legitimate device's token, also known as personification attacks. The server always checks if the combination of MAC address and token match its authentication database. Figure 4 depicts an example of the authentication and authorization log which may be viewed by system administrator.

As soon as data is successfully transmitted, the mote device shows a success icon on device's display and begins to collect consumption data again, updating the display every 5 seconds with the most recent measurement and summing up the consumption until another 5 minute window is completed, so new data is sent to the server. Once the volume of water usage of the last 5 minutes is received in the server, the total consumption is also calculated and stored with the date and time when data is received.

The SPARC server receives data from the water metering motes and stores the ID of the associated device, last collected volume of the device, total collected volume of the device and the date and time (UTC-0) which the server received the data, as shown in I. Such data comprise a reliable source for analysis services, enabling to predict consumption, water leaks and make better decisions about how we use our water resources. If false measurements were introduced my malicious users, the management of the affected facilities would be severely affected, disturbing the capture of a real picture of consumption patterns in that environment, causing waste of time searching for non-existing anomalies or delaying the detection of actual leaks and other problems. Our secure method for device register and data transmission also prevents dangers from accepting transmissions from any host in the network, which could facilitate server intrusion.

Some performance tests were proposed in order to measure the maximum capacity (throughput) at server and client-side devices. For such an experiment, an ESP8266 microcontroller

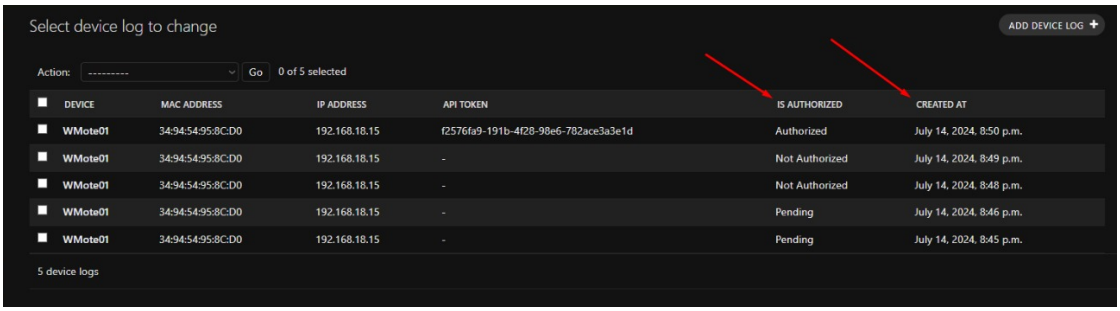

Fig. 4. SPARC authentication log

	Device ID	Last Collected (L)	Total (L)	Date and Time
01	1	0.07	0.07	15/06/24 18:45
02	1	0.33	0.4	15/06/24 18:50
03	1	0.10	0.5	15/06/24 18:55
04	1	0.6	1.1	15/06/24 19:00
05	1	0.05	1.15	15/06/24 19:05

TABELA I
EXAMPLE OF DATA RECEIVED BY THE SERVER

was configured as the client (monitoring mote device) and a Raspberry Pi 3 model B was configured as the server, considering a fog computing context.

The ESP8266 device has managed sending up to 15 requests per second to the server. Raspberry server has observed a 20% peak of CPU utilization and an increase of 12% in memory usage. The server was able to process up to 85 requests/s. Finally, in this environment, the MySQL Database was used, due to its versatility and robustness. However, Django supports other models such as MongoDB, Postgress, and MariaDB.

V. CONCLUSION

Even though the project has a solid foundation built, we are always looking for improvements. In this way, some of the future improvements are the support for multiple sensors on the same device and an smaller version of the prototype, without the Oled Display.

Another feature that we are planing to add is an SD card integration. This way, that will be possible to store the collections temporarily locally and handle connection problems, sending unsynced collections when reestablish the internet connection. This feature will require us to migrate the responsibility for handling date and time from the server to the mote.

In this way, such technology can directly and indirectly influence the conservation of the environment. Additionally, it encourages the innovation of similar technologies with the same approach. Since it is a sustainability-focused project, the source code of the project can be found on GITHUB - https://github.com/Morea-IFS/morea-ds-web - as a way to encourage and mainly spread sustainable ideas through technology.

REFERÊNCIAS

[1] ONU, "Agenda 2030 para o desenvolvimento sustentável," Disponível em: https://brasil.un.org/pt-br/91863-agenda-2030-para-o-desenvolvimento-sustent%C3%A1vel. Acesso em 27/07/2023, 2015.
[2] E. Koncagül, M. Tran, R. Connor, and S. Uhlenbrook, "The united nations world water development report 2019: leaving no one behind, facts and figures," UNESCO World Water Assessment Programme, Tech. Rep., 2019, available at https://unesdoc.unesco.org/ark:/48223/pf0000367276.
[3] ONU, "25% da população mundial não tem acesso a água potável," Available at: https://brasil.un.org/pt-br/204766-25-da-popula%C3%A7%C3%A3o-mundial-n%C3%A3o-tem-acesso-%C3%A1gua-pot%C3%A1vel-alerta-onu, 2022, accessed at 2023-08-28.
[4] UNICEF, "Water security for all," Avaialable at https://www.unicef.org/media/95241/file/water-security-for-all.pdf, 2021, accessed at 2024-09-21.
[5] M. Rodell and B. Li, "Changing intensity of hydroclimatic extreme events revealed by grace and grace-fo," *Nature Water*, vol. 1, 03 2023.
[6] BRASIL, "Lei nº 6.938, de 31 de agosto de 1981," Available at: https://www2.camara.leg.br/legin/fed/lei/1980-1987/lei-6938-31-agosto-1981-366135-publicacaooriginal-1-pl.html, 1981, accessed at 28/08/2023.
[7] U. Nations, "Human rights to water and sanitation," Avaialable at https://www.unwater.org/water-facts/human-rights-water-and-sanitation, 2024, accessed at 2024-09-21.
[8] Sistema Nacional de Informações sobre Recursos Hídricos, "Conjuntura dos recursos hídricos 2023," 2023, accessed: 2024-09-21. [Online]. Available: https://www.snirh.gov.br/portal/centrais-de-conteudos/conjuntura-dos-recursos-hidricos/conjunturainforme2023.pdf
[9] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.
[10] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.
[11] P. A. F. . R. P. V. B. Gomes, F. S., "Prototyping a solution to promote energy efficiency in smart environments using iot." *Brazilian Journal of Development*, pp. 2–8, 2020.
[12] L. A. SILVA, "Os impactos da adoção de tecnologias da indústria 4.0 nas dimensões económica, social e ambiental da sustentabilidade em empresas industriais," pp. 17–18, 2023.
[13] T. R. Fraga, "Sistema de monitoramento de consumo de água de baixo custo com comunicação wi-fi aplicado à iot." Disponível em: http://www.monografias.ufop.br/handle/35400000/3449; Acesso em 27/07/2023, pp. 2–8, 2021.
[14] R. Alves, "Solução de monitoramento de consumo de água residencial," pp. 8–25, 2015.

[15] C. Moura, R. Sousa, and J. F. Borin, "IoT aplicado ao monitoramento inteligente de distribuição de Água," Prefeitura da Unicamp, Tech. Rep., 2019. [Online]. Available: https://smartcampus.prefeitura.unicamp.br/pub/artigos_relatorios/Rafael-IoT_Aplicado_ao_Monitoramento_Inteligente_de_Distribuicao_de_Agua.pdf

[16] A. Amurim, J. Silva, M. Ortiz, P. Rego, and J. Souza, "Uma solução de iot baseada no fiware para gerenciamento de recursos energéticos e serviços acadêmicos em um campus universitário," in *Anais do V Workshop de Computação Urbana*. Porto Alegre, RS, Brasil: SBC, 2021, pp. 265–278. [Online]. Available: https://sol.sbc.org.br/index.php/courb/article/view/17119

[17] T. Nandy, M. Y. I. B. Idris, R. Md Noor, L. Mat Kiah, L. S. Lun, N. B. Annuar Juma'at, I. Ahmedy, N. Abdul Ghani, and S. Bhattacharyya, "Review on security of internet of things authentication mechanism," *IEEE Access*, vol. 7, pp. 151 054–151 089, 2019.

[18] M. Almulhim, N. Islam, and N. Zaman, "A lightweight and secure authentication scheme for iot-based e-health applications," *International Journal of Computer Science and Network Security*, vol. 19, no. 1, pp. 107–120, 2019.

[19] Django Software Foundation, "Django." [Online]. Available: https://djangoproject.com

[20] P. Leach, M. Mealling, and R. Salz, "Ietf rfc 4122. a universally unique identifier (uuid) urn namespace," Available at: https://datatracker.ietf.org/doc/html/rfc4122, 2005, accessed at 2024-07-01.