applied sciences

MDPI

Article

Leveraging IoT Harmonization: An Efficacious NB-IoT Relay for Integrating 6LoWPAN Devices into Legacy IPv4 Networks

Edgar Saavedra *, Asuncion Santamaria, Guillermo del Campo and Igor Gomez

CeDInt-UPM, Universidad Politécnica de Madrid, Campus de Montegancedo, 28223 Pozuelo de Alarcón, Spain; asun.santamaria@upm.es (A.S.); guillermo.delcampo@upm.es (G.d.C.); igor.gomez@upm.es (I.G.)
* Correspondence: e.saavedra@upm.es

Featured Application: This novel approach provides a seamless, straightforward means to make 6LoWPAN devices—pragmatically any kind of incumbent from IPv6-based IoT networks—more accessible under the scope of the omnipresent, classic IPv4 Internet.

Abstract: The burgeoning complexity and heterogeneity of IoT networks, coupled with their rapid growth, constant evolution, and new players, present significant challenges in terms of connectivity, interoperability, management, and usability. These networks, composed of a diverse array of devices, technologies and the like, demand innovative solutions to bridge the gaps between different IoT technologies and communication protocols. This article presents a simple, yet efficacious communication Relay to address one of these critical gaps. This Relay uses NB-IoT to ease the integration of 6LoWPAN-based IoT devices (IPv6) into the public legacy Internet (IPv4). This device translates 6LoWPAN, IPv6 CoAP messages into Internet-standard REST requests, so that appropriate handling of devices' data be achieved in several stages. Thus, the Relay establishes two branches of communications: (i) the local network where the 6LoWPAN gateway is placed, and (ii) the public NB-IoT network. User interaction and data analysis are achieved by virtue of Home Assistant, where former 6LoWPAN devices are now discovered and shown as proper Home Assistant entities thanks to the Relay's ease of integration into the open-source platform. This novel approach not only ensures efficient data and network management, but it also meets the urgent necessity for advanced solutions in enhancing actual IoT interconnectivity and monitoring. The unprecedented pace at which IoT devices, players and different networks have been proliferating in recent times is not compatible with countless manufacturer-dependent platforms, applications, and proprietary protocols that the IoT field has been leading with so far, almost from its beginnings.

Keywords: IoT; LPWAN; NB-IoT; 6LoWPAN; LTE; home assistant; IPv6; wireless communications; wireless sensor networks

Citation: Saavedra, E.; Santamaria, A.; del Campo, G.; Gomez, I. Leveraging IoT Harmonization: An Efficacious NB-IoT Relay for Integrating 6LoWPAN Devices into Legacy IPv4 Networks. *Appl. Sci.* **2024**, *14*, 3411. https://doi.org/10.3390/app14083411

Academic Editors: Christos Markides, Achilleas Achilleos and Georgia Kapitsaki

Received: 9 March 2024
Revised: 31 March 2024
Accepted: 6 April 2024
Published: 18 April 2024

1. Introduction

In the era of the Internet of Things (IoT), the unprecedented proliferation of devices connected to the Internet has made them omnipresent. These devices, ranging from simple sensors to complex systems, are increasingly becoming the backbone of many critical applications across various sectors, including healthcare, agriculture, driving, smart cities, or industrial automation [1].

Nonetheless, the diversity of IoT technologies, including different communication protocols and network standards, poses significant challenges in achieving seamless interoperability. Specifically, the integration of 6LoWPAN (IPv6-based) devices within legacy IPv4 networks—classical internet networks—remains a critical hurdle, hindering the realization of the full potential of IoT applications [2,3].

The transition from IPv4- to IPv6-based computer machinery and networking has not been accomplished yet, with no real coexistence between the two [4–6]. In fact, there

are still several foundational issues to address for this movement to be completed, such as the following: (i) providing support and compatibility for certain operating systems, hardware and platforms; (ii) resolving unstable routing or name services; and (iii) managing discordant security policies.

The situation is not very different in the IoT scope, and is even worse. IoT devices used to count on fewer resources; they have less ease of expansion, and lack up-to-date, long-term service usage. Moreover, the heterogeneity and vast number of IoT devices exacerbate the challenges associated with achieving a seamless transition and interoperability between IPv4 and IPv6 in this very field [7–9]. This is compounded by the diversity of communication protocols that are unique to IoT ecosystems, which further complicate the will to integrate.

Thus, it is of paramount importance to deploy devices/systems that not only facilitate communications between IPv4 and IPv6 networks, but also address the unique constraints and very protocols of IoT devices. Such solutions require innovative, yet simple approaches to ensure compatibility among players, whilst providing efficacious, reliable connectivity in a greatly heterogeneous, resource-constrained environment.

1.1. Addressing the Unforeseen, Long-Term Byproducts

The significance of interoperability in the IoT cannot be overstated. This not only ensures that devices from different manufacturers can communicate with each other, but also facilitates the development of scalable, flexible, and more efficient IoT ecosystems. Despite the advances in networking technologies, the coexistence of IPv6-enabled devices—such as those based on 6LoWPAN—with the prevailing IPv4 infrastructure, presents a complex challenge. For decades, this challenge has been compounded by the fast evolution of IoT devices and the continuous invention of new technologies, techniques, solutions, protocols, and systems [9,10].

This study promotes a simple, novel, efficacious approach to address the interoperability challenge between 6LoWPAN and IPv4 networks through the design of a simple narrowband IoT (NB-IoT) Relay. This Relay performs as a bridge, enabling 6LoWPAN devices to communicate within legacy IPv4 networks seamlessly; at the same time, the former become visible within the all-IPv4 world. However, the approach of this research is not a tunnel. Tunneling solutions tend to be patches meant to overcome the lack of supporting hardware or compatible software, thereby providing IPv6 talkability to prevent isolation [11,12]. The Relay we propose, on the other hand, does not masquerade packets to make them compatible, but performs protocol translation for the sake of actual interoperability.

Our solution is not only simple, hassle-free, and cost-effective, but also offers an accountable method for data communication by translating 6LoWPAN, IPv6 CoAP messages into standard IPv4 RESTful requests. By facilitating this translation, the relay ensures that 6LoWPAN devices can be integrated into existing network infrastructures without significant changes or upgrades. This fact is crucial, considering the large number of infrastructures that may be dependent on IoT networks functioning properly, which would otherwise require significant analysis and costs to overhaul.

Using the NB-IoT offers several advantages such as wide coverage, high power efficiency, and agnostic infrastructures. These matters make the NB-IoT an ideal choice for IoT applications that require little human interaction, as well as those that are expected to be deployed in very heterogeneous and diverse use cases and locations [13,14]. Furthermore, the integration of the Relay with a Home Assistant (HA) [15,16], a state-of-the-art, open-source, *home-and-beyond* automation platform, exemplifies the practical application of the proposed solution, demonstrating its effectiveness in real-world scenarios, as well as our commitment to open sourcing.

1.2. Previous Literature

Given the unique nature of this project and the recent actual emergence of the NB-IoT, identifying case studies with similar objectives and complexities proved to be challenging. This project's distinctive problem statement and the incorporation of a broad range of apparently distant technologies span multiple areas of specialization. Nevertheless, there are a few projects worth mentioning—projects that embarked on facilitating this transition we are targeting.

One such initiative, as presented by Da Silva et al. in [17], aimed at the "Design and Construction of Wireless Sensor Network Gateway with IPv4/IPv6 Support". This project's primary objective was to develop a communication gateway facilitating bidirectional exchanges between IPv4/IPv6 clients and a 6LoWPAN sensor network. This endeavor involved setting up a 6LoWPAN sensor network using TinyOS-operated communication motes. The implementation leveraged TinyOS's BLIP protocol for IPv6 communication over IEEE 802.15.4 wireless links, complemented by client applications for both IPv6 and IpPv4 to request sensor readings from specific network nodes. The outcomes affirmed the gateway's capability to ensure interoperability between IPv6/IPv4 clients and the sensor network, enabling direct interactions with the sensor nodes.

Another interesting and novel approach, conceptually similar to ours, is that proposed by Arzo et al. in [18], who introduced a network format translator into a virtualized environment. This approach aims at bridging the gap between different IoT networks, enabling seamless communication across various technology platforms. By implementing a testbed utilizing the NS3 simulator, the study demonstrated the feasibility of communicating across different IoT technologies, such as transmitting packets between LoRaWAN, Wi-Fi, and 6LoWPAN networks. Nonetheless, it is worth noting that this approach does not focus on the actual, hassle-free IoT interoperability, but feasible technical realization—they did not carry out an actual test with in-the-flesh networks, but a simulation thereof using NS3.

Furthering the exploration into IPv6/IPv4 gateway implementations, another noteworthy project is "Network Processors Applied to IPv4/IPv6 Transition", as discussed by Grosse et al. in [19]. This research introduced a high-speed IPv6/IPv4 gateway utilizing network processors, which focuses on handling substantial traffic volumes and facilitating network address, port, and protocol translation (NAPT-PT) between IPv6 and IPv4 networks. The study detailed significant performance enhancements over conventional computer/server-based implementations, and addressed the limitations concerning network address and protocol translation and firewall processing compared to general-purpose processors.

Additionally, "A SOCKS-Based IPv6/IPv4 Gateway Mechanism", documented by Kitamura in [20], describes a SOCKS protocol-based IPv6/IPv4 gateway mechanism enabling seamless communication between IPv6 and IPv4 nodes. This mechanism supports heterogeneous communication and the forwarding of IPv4 and IPv6 connections at the application layer, without introducing new protocols or compromising existing communication functionalities. The resulting SOCKS-based IPv6/IPv4 gateway mechanism facilitates heterogeneous communication and connection forwarding, maintaining the SOCKS mechanism's communication environment without necessitating DNS system modifications or alterations to existing applications, thanks to sockification through a SOCKS library installation on the nodes.

On top of that, surveys like Ghumman's [21] delve into IPv4/IPv6 transition, exploring the most important methodologies such as dual stack, tunneling, and network address translation protocol translation, with their respective impacts on IoT infrastructure. Ghumman's research highlights the intricacies of IPv6 transition methods and their potential to address the burgeoning demands for IP addresses in the IoT realm. The research also emphasizes the difficulty of implementing real translators, mainly due to the great diversity of devices and few resources available. This survey underscores the importance of IPv6 for enhancing IoT security, scalability, and connectivity, marking a critical step towards the future of Internet protocols and their application within the IoT ecosystem.

These examples represent the most current, closest approaches in the endeavor to implement a gateway or Relay. While each project bears unique features, they collectively underscore the research domain's focus on creating and implementing communication gateways between these two pivotal technologies, highlighting the field's ongoing relevance and the imperative for advanced solutions in promoting IoT interconnectivity. It is worth noting that all of the projects share a common goal: to facilitate and optimize communication between different network protocols, evidencing the evolution of research in this area, although the NB-IoT seems to be the least-represented research in this field so far.

Hence, the device presented in this study contributes to the growing body of literature on IoT interoperability by providing a simpler, easier, yet reliable solution to a pressing problem. Previous research in this area focused on various aspects of IoT communications, but the use of future-proof NB-IoT as the main communications layer to cross the bridge adds another dimension to the discourse—as a new, unique approach to aid the integration of 6LoWPAN devices into IPv4 networks. As the IoT landscape continues to evolve, the significance of developing interoperable solutions that can adapt to the changing technological environment cannot be underestimated.

In conclusion, we not only present a novel solution to a critical challenge in IoT interoperability, but also highlight the importance of simplicity and efficacy in the design of communication relays—or gateways. The findings of this study are expected to have significant implications on the development of future IoT networks, paving the way for more integrated, versatile, user-friendly IoT ecosystems.

1.3. Article's Structure

The rest of the paper is organized as follows:

Section 2 explains the significant, basic issue with the IoT field, which is the enormous variety of devices, protocols, technologies, manufacturers, etc., as well as this field's slow, step-by-step evolution for more than a decade. It has leveraged a wide range of heterogeneous use cases and devices, thereby dragging interoperability and universal deployment barriers. The two big players in the game are explained, 6LoWPAN and NB-IoT, alongside their matching upper-layer protocols, namely CoAP and REST; we also describe our approach to overcome to this issue, so that the reader can appreciate the Relay's scope; finally, Section 2 explains our vision on HA as an essential enabler in IoT harmonization.

Section 3 presents the Relay itself and its abstraction working schemas, focusing on its main components, keys, and distinct primary resources—both hardware and software—as well as specific things that were tailored for its development and actual implementation in a real-world scenario, highlighting the main issues encountered during this stage, as well as the primary outcomes of interest.

In Section 4, we conclude the satisfactory results of our Relay, highlighting this type of research's importance in the pursuit of a real, profound IoT blending in society. To finalize, we discuss security concerns and future sights on the long-term IoT paradigm.

2. The Elephant in the Room: Great Diversity

In addressing the multifaceted domain of the Internet of Things, a critical, often overlooked issue emerges as *the elephant in the room*: the pervasive challenge of interoperability across a rapidly expanding and evolving network of devices. This challenge is not merely a technical inconvenience, but a fundamental barrier to realizing the IoT's transformative potential. Interoperability—or lack thereof—affects everything from user experience and system efficacy to the scalability and adoption of IoT solutions on a global scale.

Despite the increasing acknowledgment of its importance, the nuanced complexities and underlying technological disparities that contribute to interoperability challenges remain underexplored. In the ensuing subsections, we delve into the core aspects of these challenges, ranging from protocol diversity and network compatibility to the integration hurdles posed by legacy systems and emerging standards. By dissecting these issues, we

aim to lay a comprehensive foundation for understanding the critical need for innovative solutions that can bridge these gaps, thus setting the stage for the novel contributions of our research.

2.1. One Simple Approach to Help Harmonization

The primary objective of this paper is to develop and implement a solution to connect and expose data from IoT sensors to the Internet, based on the 6LoWPAN protocol. This solution involves creating a communications Relay that allows leaf nodes in the network to communicate with the cloud. This Relay device would host a two-way communications system: (i) a local area network, to speak with the 6LoWPAN coordinator, and (ii) NB-IoT, which provides the transparent, logical-direct path to the cloud platform where data are integrated.

6LoWPAN sensors usually exchange information using the CoAP protocol. Network coordinators usually use their own methods, platforms, or *secret recipes* to subsequently make these data appear somewhere else where access is granted (IPv4 networks). However, this layer is usually opaque and tailored specifically for the very brand/use case itself, with little to no chance of modification.

To overcome this issue, we propose a new type of *Thing* based on a low-cost FiPy module [22]. This development board comes handy, as it runs on the well-known ESP32 family of chips, and it incorporates Wi-Fi for the local access path, NB-IoT for the global path, as well as some other wireless technologies such as BLE, Sigfox, and LoRa. The main architecture of the system can be seen in Figure 1.

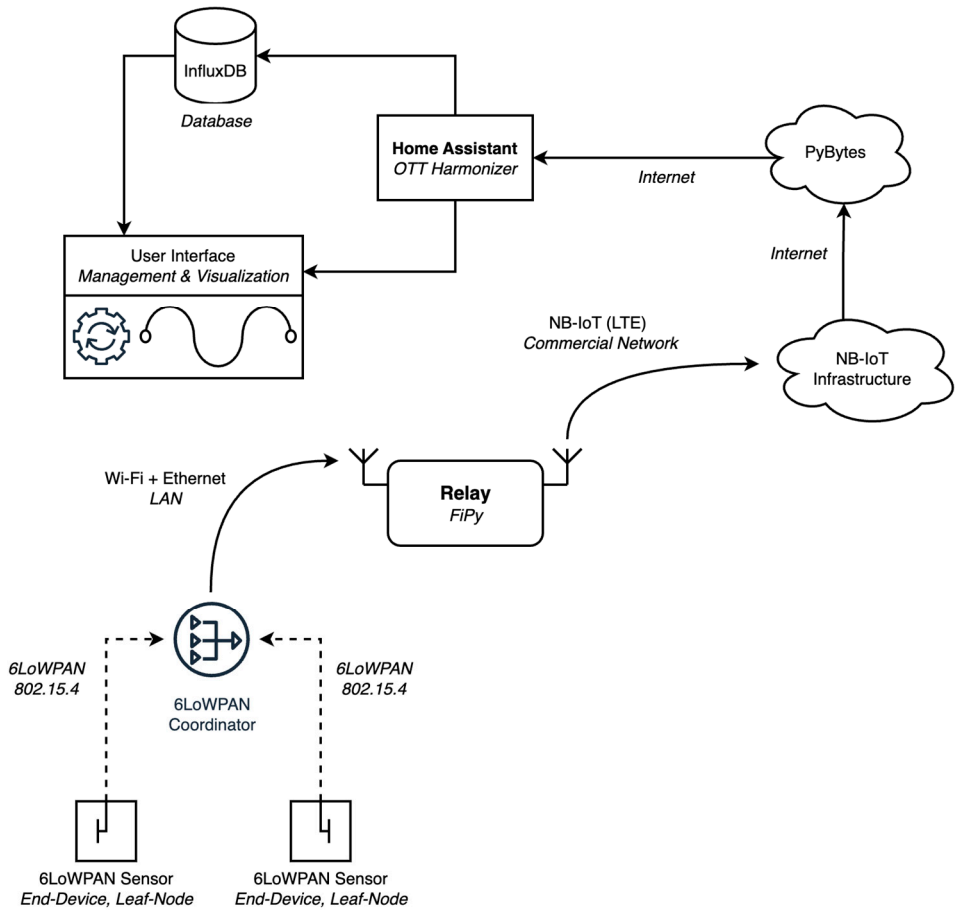

Figure 1. General block diagram for this project's architecture.

Thus, data would be requested to the 6LoWPAN coordinator by the Relay, which afterwards properly parses the data as a JSON document, then uploads it to the cloud.

Notice that there is a middleware platform in between called PyBytes [23]. Although this could be avoided, it is the most straightforward manner to use NB-IoT with Pycom development boards.

Furthermore, this approach is almost carrier agnostic, leveraging ubiquity and ease of implementation. Only two parameters are to be set in the Relay's program code, the APN and LTE band. However, in Europe, the band is often FDD #20 (~800 MHz), regardless of the mobile carrier and country, and the APN is a static parameter per carrier. With this, the developer only needs to invoke Pybytes' library functions to send messages to the back end.

The LTE modem scans the designated band, and then attaches to the very narrow-band carrier commanded by the network, which may change its central frequency between geographical locations, even inside the same country and mobile operator. For this research, 1NCE [24] was chosen as the mobile carrier, which was actually using Vodafone's NB-IoT towers/network; they are just a reseller providing quasi-global NB-IoT service.

Once attached and connected to the cellular network, the Relay can successfully send data to Pybytes, which then sends these data directly to the Home Assistant API to accordingly store and cure the incoming data on the InfluxDB database, eventually triggering automations or whatsoever, should they be set up.

In summary, this study presents a comprehensive solution for the collection, processing, transmission, and exposure of IoT sensor data to the Internet, utilizing leading-edge, open-source technologies, and ensuring a new roadmap for work in the coming years, offering high interoperability thanks to the use of standard protocols in the IoT industry.

To prove the Relay's proper functioning, we set up a simple indoor testbench in a medium-sized room with a typical setup composed of the following: (i) a 6LoWPAN network with one coordinator node and two ambient sensor nodes; (ii) the Relay itself, centered on the FiPy board, which embeds the NB-IoT modem; and (iii) a Wi-Fi router, providing LAN/WLAN connectivity between the coordinator node and the Relay device. Apart from this reachable set up, there were also an AWS-Lightsail server where the Home Assistant instance was deployed, exposing the endpoint to which Pybytes would forward NB-IoT messages, and providing the web interface for the user to visualize data and interact with the system.

2.2. 6LoWPAN

In the realm of the Internet of Things (IoT), enhancing energy efficiency and connectivity in various environments necessitates innovative networking solutions. Devices in these networks are often interconnected in a mesh topology, leveraging an adaptation of the 802.15.4 standard through 6LoWPAN. 6LoWPAN, standing for IPv6 over Low-Power Wireless Personal Area Networks, is pivotal for enabling devices with constrained processing and power resources to communicate over the IPv6 protocol, thus offering notable advantages such as interoperability and flexibility. The protocol's extensive addressing structure, provided by IPv6, significantly aids in scaling IoT networks by facilitating the addressing of a virtually unlimited number of devices.

Moreover, 6LoWPAN's efficiency in bandwidth utilization is achieved through header compression mechanisms. This efficiency is crucial in reducing the size of transmitted data packets, an essential feature in wireless sensor networks where transmission capacity and battery longevity are of paramount importance. Consequently, the application of 6LoWPAN in IoT device communication propels the interoperability, scalability, and efficiency of deployments, facilitating the establishment of comprehensive networks.

The integration of 6LoWPAN with NB-IoT represents a strategic advancement that capitalizes on the strengths of both technologies. The NB-IoT is celebrated for its exceptional coverage, power efficiency, and reliability, providing a reliable communication layer for IoT devices in scenarios where traditional connectivity options are impractical or overly power consuming. This symbiosis between 6LoWPAN and NB-IoT enhances the seamless and efficient transmission of data from localized, star-of-stars IoT networks to the broader

Internet, effectively narrowing the divide between localized IoT networks and the expansive global Internet infrastructure. Such integration is essential for the development of IoT systems that are scalable, interoperable, and capable of efficient operation across diverse environments and protocols, marking a significant step towards the realization of fully connected and efficient IoT ecosystems [3,25,26].

There are at least two main types of devices expected in 6LoWPAN networks: (i) coordinators and (ii) leaves. Our testing scenario is composed of one coordinator node and two leaves, as follows:

The coordinator node (see Figure 2, left), centered on a BeagleBone Black, offers a robust platform for managing network communications and data processing tasks. This single-board computer's significant processing power and connectivity options make it ideal for overseeing the operations of an IoT network. The coordinator node is enabled by a 6LoWPAN standard communication module, establishing it as the network's central hub. Notably, the BeagleBone Black implements a CoAP (Constrained Application Protocol) server, designed to handle request-based communications from the network's sensor nodes. This setup is pivotal for managing the energy-efficient protocol operations, ensuring that data are relayed efficiently from the sensor nodes to the coordinator, and then onwards as required. The 6LoWPAN device connects to the BeagleBone via UART. This connection method is instrumental in maintaining the system's overall low power consumption and simplicity, whilst ensuring a low-data-rate, seamless stream from the capillary network.

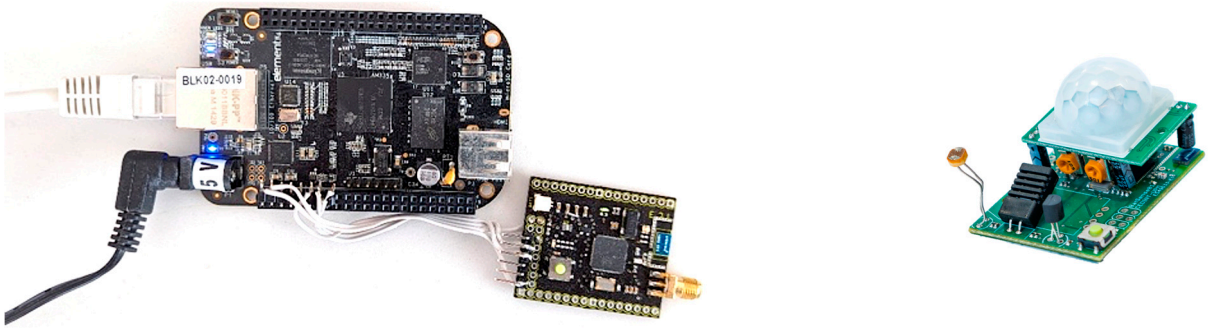

Figure 2. Left: coordinator node: BeagleBone Black + 6LoWPAN border–router node; **right**: ambient sensor nodes used in this project.

Standard/leaf nodes (see Figure 2, right) were deployed, which in the scope of this study happen to be ambient sensors, although any kind of device would be set the same way. Parameters gathered by ambient sensors are typical IoT parameters—temperature, humidity, luminosity, and motion—so they seemed to be a good choice to implement for testing. In alignment with the principles of low power consumption and efficient communication, these ambient sensors utilize a request-based CoAP. This protocol is specifically tailored for constrained devices like ours, allowing them to operate on minimal power by only activating when sending or receiving data as needed. These sensors' design reflects a meticulous balance between power efficiency and operational capability, ensuring that even with their limited energy resources, they provide reliable data transmission.

2.3. NB-IoT

Cellular networks have been a cornerstone in the evolution of communications over the past few decades, offering uninterrupted connectivity almost anywhere in the world. From their early versions, which primarily supported calls and text messages, to modern high-speed networks facilitating data, video, and other multimedia applications, they have transformed how we communicate and access information.

However, with the increasing need to connect with people as well as devices within the Internet of Things, there emerged a requirement for specific technologies that could

adapt to these new demands. In this study, the narrowband IoT (NB-IoT) comes into play as a solution based on cellular networks [27–34].

As a modern and meticulously designed technology, the NB-IoT stands out as the optimal solution tailored to meet the specific needs of IoT communication networks. Its recent development allows it to surpass other technologies by optimizing every facet, thus ensuring superior efficiency and performance in the IoT realm. The NB-IoT's youth and thoughtful development make it perform well in its scope. This advantage is further bolstered by the backing of telecommunications operators, who ensure long-term support by investing heavily in this technology. Such investments have made the NB-IoT remarkably affordable and accessible for a wide range of applications. We consider the NB-IoT to be an optimal technology for a wide range of IoT use cases, as explained in the next subsections.

2.3.1. Global, Carrier-Grade Network

The advent of the NB-IoT marks a significant milestone in the evolution of global, carrier-grade networks, offering a robust solution for extending IoT connectivity across a myriad of devices worldwide. Engineered to operate within the licensed spectrum, the NB-IoT benefits from the ease-of-use, reliability, and security that are inherent to carrier-managed networks, ensuring stable and secure communications for IoT devices, even in the most challenging environments. In addition, licensed bands augment its resilience to external attacks, QoS, and general control over the network's lowest layers.

Its unique capacity to penetrate deep into buildings and underground areas, mainly due to its usual functioning on sub-gigahertz bands, makes it an ideal choice for a wide range of applications, from smart metering in utilities to asset tracking in logistics. Moreover, the NB-IoT's highly efficient power usage can extend devices' battery lives for years, reducing the maintenance costs associated with IoT deployments.

As part of the global LTE standard, the NB-IoT enjoys widespread international support from telecom operators, facilitating seamless, cross-border IoT solutions and driving forward the vision of a fully interconnected world. The global reach and carrier-grade reliability of the NB-IoT stand as pillars for the next wave of IoT innovation, enabling a new realm of applications that were previously untenable due to connectivity and power constraints. In the specific case of Spain, where this research was carried out, the three largest carriers (Telefónica, Vodafone, Orange) provide virtually full NB-IoT coverage over the whole population. This fact is vital for enabling solutions for a wide variety of scenarios, especially considering that a single NB-IoT sector, usually three sectors per cell, can operate more than 100,000 devices [35].

2.3.2. Low-Power Communication Technology

The NB-IoT stands out in the realm of low-power wireless communication technologies due to its exceptional capabilities that are specifically tailored for the modern IoT. Standardized by the 3GPP in Release 13 back in 2016, the NB-IoT was meticulously crafted to support the burgeoning demand for a network that can efficiently connect a vast number of devices across extensive areas without the burden of high energy consumption. By leveraging a narrow bandwidth of around 200 kHz for its transmissions, The NB-IoT is not only able to ensure low-speed data exchange, but also significantly extends the battery life of IoT devices, making it an indispensable technology for scenarios where devices are expected to operate for years without battery replacement.

The NB-IoT's design focuses on minimal energy usage, while still providing robust and reliable connectivity. This is particularly advantageous for a wide array of IoT applications that necessitate prolonged device longevity. Its enhanced coverage and deep penetration capabilities make it perfectly suited for monitoring environmental factors in remote or difficult-to-access locations [36].

The advent of the NB-IoT as a low-power communication technology marks a pivotal advancement in the IoT ecosystem. Its ability to offer extensive coverage, superior indoor penetration, and ultra-low energy consumption while leveraging existing cellular network

infrastructures makes it an ideal candidate for a plethora of IoT applications. This positions the NB-IoT as a cornerstone technology in the ongoing evolution of smart cities, agriculture, environmental monitoring, and beyond, heralding a new era of connectivity that is both efficient and sustainable.

2.3.3. Streamlined for IoT—An LTE Evolution

The evolution of the NB-IoT on an established technology like LTE, and its implementation over a licensed frequency spectrum, optimizes network capabilities, relieving devices of hardware and software complexity demands. Adoption of the NB-IoT is further propelled by its integration into existing cellular network infrastructure, allowing for its cost-effective rollout and seamless scalability. It can be deployed on a GSM (2 G) channel, on 4 G guard-band space, or on the standard 4 G/5 G spectrum and equipment [31]. This integration ensures that the NB-IoT benefits from the established security and reliability features of cellular networks, as well as their carriers' know-how, providing a secure, efficacious communication channel for transmitting sensitive information.

Despite being derived from LTE specifications, the NB-IoT standard was designed to maintain as simple a communication interface as possible, aiming to lower device manufacturing costs and minimize battery consumption. Many LTE features that are unnecessary for IoT services have been omitted in the NB-IoT, such as handover for voice quality, carrier aggregation for signal quality enhancement, and dual connectivity for multi-carrier communication.

2.3.4. Frequency Band Utilization and Messaging

The NB-IoT's strategic approach to frequency band utilization significantly enhances its applicability across a broad spectrum of IoT deployments. It operates in three distinct modes: (i) in-band, utilizing the LTE carrier blocks; (ii) guard-band, leveraging the unused spectrum in LTE guard bands; and (iii) stand-alone, repurposing existing GSM frequency bans; in so doing, the NB-IoT exhibits unparalleled flexibility in network implementation. This flexibility is critical in densely populated urban environments as well as in rural areas, where spectrum efficiency and coverage requirements vary greatly.

The architecture of the NB-IoT was meticulously engineered to support the transmission of small data packets, corresponding to periodic updates from IoT devices. The NB-IoT's design specifically addresses IoT requirements, enabling its efficient management of compact data packets. This efficiency is critical for applications that require frequent updates from a vast array of devices, such as utility meters, environmental sensors, and health monitors, ensuring that the network remains uncluttered and responsive.

The NB-IoT provides a solid foundation for wide-area IoT applications, which, combined with 1600-byte messages, makes the NB-IoT a highly versatile technology. It not only caters to dense, complex urban environments, but also extends its benefits to remote, underserved rural locations, where connectivity has traditionally been a challenge.

2.4. Protocols Involved within the Application Layer: CoAP and REST

In the IoT ecosystem, ensuring efficient communication between devices is pivotal. Among the protocols tailored for the IoT, CoAP and REST stand out for their utility in constrained environments and web-based applications, respectively.

2.4.1. CoAP: Constrained Application Protocol

CoAP is a lightweight protocol designed for machines. It is akin to a compact version of HTTP for devices with limited resources, using a straightforward model for sending and receiving messages. Unlike HTTP, it operates over UDP, making it better suited for the minimal power and processing capabilities of IoT devices. CoAP supports interactions in IoT applications that require minimal bandwidth and energy consumption [37].

2.4.2. REST: Representational State Transfer

REST leverages the existing HTTP infrastructure to create or access resources using standard HTTP methods. It is widely adopted for web APIs, enabling straightforward and flexible interactions with services. RESTful interfaces are favored for their scalability and ease of integration across diverse platforms, making them suitable for complex IoT ecosystems where different devices and services need seamless communication [38].

Both CoAP and REST are integral to the IoT application layer, offering distinct advantages for device-to-device and device-to-service communication. CoAP excels in constrained environments, while REST is preferred for broader web integration, highlighting the importance of selecting the right protocol based on the specific requirements of an IoT deployment.

2.5. Home Assistant: Agnostifying Data in Pursuit of a Diverse Coherence

Home Assistant (HA) technology stands as a paradigm of open-source home automation; it is designed with a strong emphasis on privacy and local control. Emerging as an antidote to the fragmentation and privacy concerns associated with proprietary or cloud-based solutions, HAs champion interoperability among diverse smart devices without sacrificing user privacy. The platform's open-source nature not only underscores its commitment to transparency and security, but also paves the way for unparalleled flexibility and customization. Users can tailor the platform to their specific needs, benefiting from the collective intelligence of a global developer community committed to advancing HA's capabilities [15,39].

Developed initially in 2013 by Schoutsen, HA's foundation in Python and open-source principles has fostered a rich ecosystem of contributions. The platform integrates a wide array of devices and services through modular components, ensuring a cohesive and customizable user experience across various devices and technologies. This inclusive architecture has facilitated the rapid adoption and continuous growth of HAs, supported by an active community and frequent updates that introduce new functionalities and integrations.

The significance of the HA community cannot be overstated. It thrives on continuous contributions of new integrations, enhancements, and fixes, serving as an invaluable resource for newcomers and experienced users alike. The platform's extensive documentation further aids users in navigating installation, configuration, and customization processes, making HA technology accessible to a broad audience.

As HA technology evolves, it consistently adapts to the burgeoning landscape of IoT devices and user expectations, ensuring its relevance in the ever-changing domain of home automation. Its dedication to privacy, localization, and flexibility, coupled with robust community support and comprehensive documentation, positions HA technology as a pivotal player in the home automation ecosystem. While originally tailored for home lab use, HA technology's adaptability hints at broader applications, including industrial settings. This exploration underscores HA technology's potential as a versatile and robust IoT management platform, extending beyond traditional home automation to encompass a wider array of environments and applications, such as emerging smart cities' platforms [40].

In fact, HAs stand at the forefront of driving the IoT's scalability and interoperability, offering a compelling model for open-source development by facilitating an expansive, community-driven approach to smart devices integration. This platform highlights the value of an open-source ethos to foster innovation, as it enables rapid integration of devices across sundry manufacturers and protocols, breaking barriers often encountered in proprietary ecosystems.

3. Relaying

In this section, we unveil the intricacies of the Relay, focusing on the essential components and resources foundational to its design. This includes an examination of both its hardware and software elements, alongside bespoke developments tailored for its construction and actual deployment. By presenting the Relay's architecture and operational

capabilities, this section aims to elucidate its role and efficiency within the broader context of IoT applications, demonstrating the Relay's simple yet efficacious functioning.

3.1. Starring Hardware

The Relay's main hardware component is the FiPy board by Pycom, an innovative choice reflecting our commitment to versatility and integration. This powerful development board supports a multitude of communication standards, including Sigfox, LoRaWAN, NB-IoT, Wi-Fi, and BLE, all within a single device. The choice of FiPy is pivotal, owing to its unique ability to navigate across various network technologies, thus facilitating seamless communication in diversified IoT ecosystems. Its dual-core 32-bit LX6 microcontroller, programmed in MicroPython, offers a flexible and efficient platform for developing IoT applications that require multi-network connectivity.

3.2. Collecting with CoAP

To address the complexities of IoT communications within a sophisticated network environment, a comprehensive solution was developed to bridge the gap between CoAP and HTTP protocols through the implementation of a RESTful micro-server. This approach was realized using Python, a language chosen for its flexibility and extensive support, and because of its presence in the core of HA technology; thus, leaner integration between them can be achieved if needed. We took advantage of Flask [41], a microframework celebrated for its minimalistic yet powerful features at the same time that it helps us accelerate web-related coding.

The backbone of this communication server is the CoAPython library [42], which plays a pivotal role in integrating CoAP protocol functionalities, facilitating seamless interactions between IoT devices. CoAP messages are accordingly parsed, as stated by the simple data model of the 6LoWPAN devices deployed in this project.

In this fashion, significant data values and sensor states can be extracted from CoAP messages, then incorporated into a more common, current, and suitable format. This process mostly involves data *JSONification* and basic modeling. This conversion process, although not intricate, is critical for ensuring that data from foreign IoT devices are discoverable, easily accessible, and manageable through common Internet web technologies. In Figure 3, the reader can see a simple diagram of the network abstracted to the upper layers that depicts the changes in protocols we are dealing with.

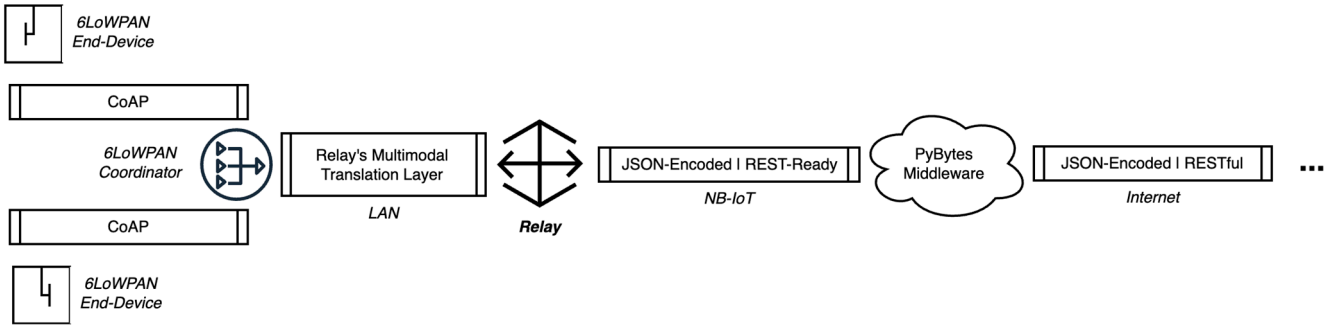

Figure 3. A coarse, protocol-oriented representation of the IoT chain.

The server architecture is designed with resource efficiency in mind, as always-first, major IoT mantra, allowing for lightweight operations that maintain system performance while handling data exchanges. Flask's ability to create a minimal yet functional web server environment has been instrumental in this regard, providing only essential components to support RESTful interactions and CoAP compliance, whilst not overwhelming the system with unnecessary matters. Moreover, the server's configuration includes a set of predefined routes, each catering to specific data retrieval or device interaction needs, as one of the main

intricacies with iPv6 networks is their routing's lack of ease and iPv4 direct compatibility, a fact that is usually worsened by the *(ab)* use of NAT and tunneling.

This structured, kind of isolated approach not only simplifies usability for developers and system integrators, but also enhances the system's reliability and scalability by clearly defining communication pathways and data processing methodologies, helping future-proofing. In our actual testing deployment, the server was connected via Wi-Fi to the same LAN as the 6LoWPAN coordinator was connected to.

The server periodically queries every IoT device comprising the designated 6LoWPAN network, as claimed by the coordinator. Note that there are also methods implemented to retrieve network characteristics from the coordinator, such as lists of devices, individual device information and sensing capabilities thereof, network telemetries and quality indexes, sensor data and states per se, etc. As stated, the server collects and organizes data into JSON documents following the appropriate models. These data are now available to be pushed to the middleware: PyBytes.

3.3. Pushing with NB-IoT

Integration of the NB-IoT into our Relay system underscores a strategic embrace of cellular technology for the IoT. Pycom provides PyBytes as the easiest, most direct connection of their own branded development boards with the cloud using, among other technologies, the NB-IoT. Nonetheless, hassle-free NB-IoT bridging is especially remarkable, as current utilization of the NB-IoT within the end-user scope is still cumbersome. Integration tends to be carrier-dependent, and documentation is scarce. In fact, carriers or vendors from whom rights to use NB-IoT communications must be acquired—usually (e)SIM cards—are hard to find.

Thus, having a carrier-agnostic middleware which masks carrier-related issues and avoids specific settings tuning is something worth highlighting. With this, once PyBytes is properly configured and the modem effectively connects to the NB-IoT's network (Figure 4), sending data to the middleware using the NB-IoT just implies using a library function in the fashion of the following:

```
...
pybytes.send(chunk)
...
```

SYSTEM FSM	STATE	SYSTEM FSM	STATE
RRC TOP FSM	SCANNING	ESM BEARER FSM	BEARER_NULL
RRC SEARCH FSM	WAIT_RSSI	SMS MT FSM	IDLE
RRC ACTIVE FSM	NULL	SMS MO FSM	IDLE
PMM PLMN FSM	NORM_WAITCELL	LPP FSM	IDLE
EMM MAIN FSM	NULL	HP MAIN FSM	IDLE
EMM AUTH FSM	KASME_DEFINED	HP USIM FSM	READY
EMM CONN FSM	NULL	HP SMS MO FSM	IDLE
EMM TAU FSM	NULL	HP SWI MT FSM	IDLE
EMM TEST FSM	NULL	HP CAT FSM	IDLE

Figure 4. AT commands (finite state machines' states) printed by the LTE modem in console when the FiPy module is authenticating in the NB-IoT network.

For the cycle to be completed and NB-IoT messages properly forwarded from PyBytes to the HA instance, rules must be defined in the middleware. These rules are evaluated every time a new message is received—messages are called Signals within the PyBytes middleware, as depicted in Figure 5.

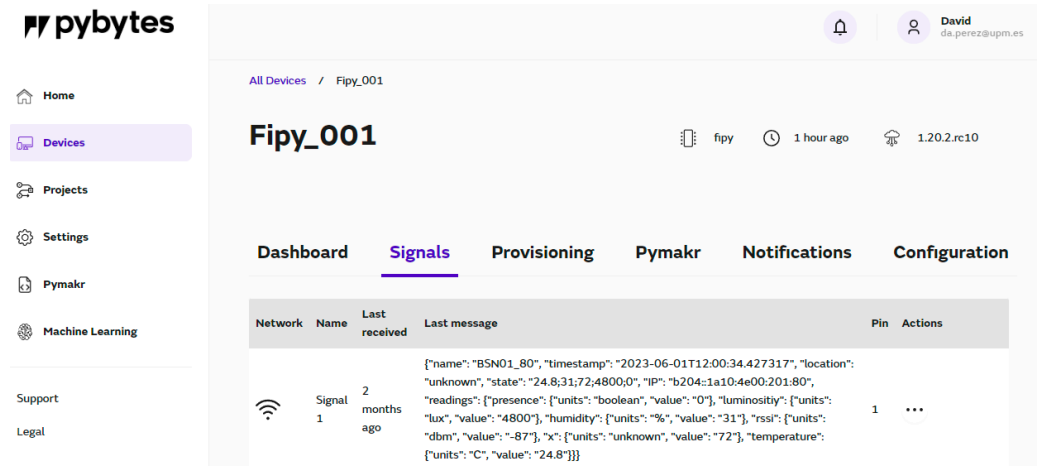

Figure 5. PyBytes' back-end displaying the so-called Signals Table The reader may see an example of one such message received from the Relay. In its structure, crucial pieces of information like the 6LoWPAN device's identification, sensing values states, and measurement timestamps can be observed.

For this project's specific case, we just checked if new messages had an identifier embedded in one specific field of the Relay's forwarded messages. If so, a POST REST request was sent to the HA API—with the proper authorization token—which would handle it accordingly and hopefully store the information received in the designated sensor states.

3.4. Pulling with Home Assistant

Connecting the Relay to the HA showcases our dedication to creating user-centric, future-proof, expandable IoT solutions. This being a specifically tailored ad hoc use case, manual sensor definition must be conducted in the HA configuration files for them to be properly integrated.

As an example, Figure 6 depicts the definition of two custom templated sensors used within this project's scope. Note that the sensors' value templating vastly varies according to the JSON data model we use in the HA API requests. In the following example, we were barely able to input the whole JSON text string into the API as an input text field, which afterward split into meaningful sensors, as shown in Figure 6.

```
sensor:
  - platform: template
    sensors:
      bs79_net:
        friendly_name: "NetID_79"
        unique_id: "sensor.bs_79_net_20230721_0"
        value_template: "{{ states('input_text.batsense_1').split(',')[0]}}"
      bs79_nameshort:
        unique_id: "sensor.bs_79_name_20072023_0"
        friendly_name: "Name_79"
        value_template: "{{ states('input_text.batsense_1').split(',')[1]}}"
```

Figure 6. Exemplification of two custom templated sensors defined in the HA's realm.

The HA's core was complemented with other modules such as Grafana for rapid, seamless data visualization and simple integration thereof. Home Assistant dashboards and other UI resources could be used to control appliances or actuator devices, as well as set certain configuration parameters.

By pulling data into the HA, users can leverage its extensive ecosystem of plugins and integrations to automate tasks, visualize data, and control smart devices, effectively

making the Relay an integral part of a sophisticated home-and-beyond automation system. A simple card displaying the data from the pair of sensors defined in Figure 6, but in a more meaningful manner, is shown in Figure 7 (left); a more complex dashboard for the same pair of sensors Is depicted in Figure 7 (right).

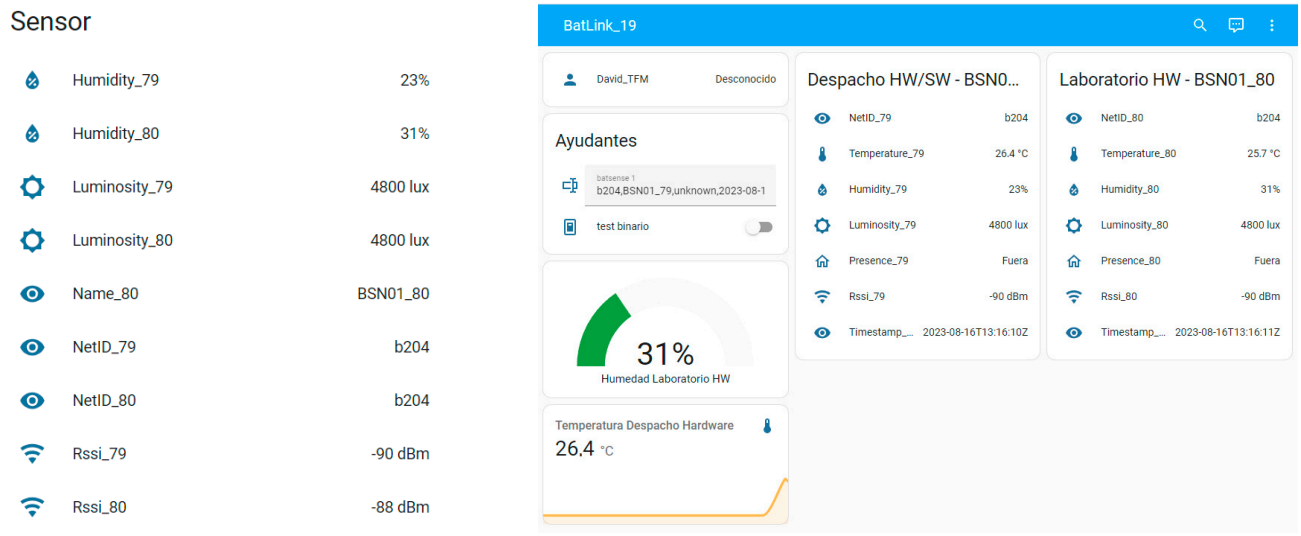

Figure 7. Two custom templated sensors natively displayed in the HA.

3.5. Storing with InfluxDB

The integration of InfluxDB within HA offers a powerful combination for home automation performance and beyond. InfluxDB, a time series database, is designed to handle high write and query loads, making it ideal for storing and analyzing vast amounts of IoT data, like those generated by an HA. These streams of data can grow easily several hundreds of megabytes per day when a handful of devices are frequently polled.

This integration allows users to efficiently log data from various sensors and devices managed by the HA, enabling detailed analysis and visualization of trends over time. Such capabilities significantly enhance the potential for optimizing home environments, energy usage, and understanding patterns in daily routines, including outliers.

InfluxDB also comes with Kronograf for data visualization and Telegraf for monitoring the database's performance, metrics, and the like.

4. Conclusions and Loose Ends

The Relay system developed through this research may serve as a pivotal stride towards achieving tangible IoT interoperability, a feat that remains largely elusive in contemporary settings. The Relay, designed with an emphasis on simplicity, ease of deployment, usability, and efficacy, empowers a broad spectrum of users to implement it with minimal complexities, thereby accelerating the realization of genuine IoT harmonization.

Through a proper selection and integration of hardware, software, and infrastructure components, including the FiPy module, the NB-IoT infrastructure and the HA ecosystem, our research met its technical objectives. At the same time, we are facilitating the real, deep integration IoT needs to become a usable part of society's daily life.

The Relay's design, highlighted by its straightforward yet thoughtfully intended implementation, underscores its innovative approach to dismantling the barriers that currently hinder seamless IoT communication. Immediate next steps involve a deeper characterization of the Relay, including time responses and latency variations due to its presence, eventual packet loss and error rate, and performance stability. So far, we carried out qualitative, naked eye evaluation procedures where it seemed to perform as expected; however, further, more precise tests must be realized, such as those carried out in [14].

Deployment of communication relays like this, as well as the adoption of standardized IoT protocols, will gain market interest in the long term. Although big players and industry leaders may initially be reticent to forego their control on proprietary systems, open ecosystems end up driving larger market and investment figures, with new, often unexpected relations among different players. This may eventually lead to enormous expenditures in the research and innovation of such fields, which big players and investors may also take advantage of.

However, the IoT is evolving rapidly, which may be an issue from a standardization perspective, as the diverse and evolving nature presents a challenge in establishing timely harmonious, global standards. To help overcome these barriers, stakeholders like standardization bodies and industry leaders must keep collaborating to foster IoT harmonization, thereby unlocking the full potential of IoT interoperability and connectivity.

By providing a clear pathway for the ad hoc development and deployment of such relays in real-world scenarios, these findings may lay a foundation for future advancements in IoT interoperability, highlighting the synergy between diverse technologies, tools, and software systems in overcoming the complexities of IoT ecosystems.

4.1. Security-Proofing—Concerns on IoT Network Reliance

Integrating communication relays into IoT networks brings to light several security challenges that are paramount to maintaining the integrity, confidentiality, and safety of data traversing these networks, as well as services dependent on them. A multi-faceted approach is necessary, including encryption, authentication, regular updates, proactive monitoring, and compliance with established security standards.

Such a strategy ensures the integrity and reliability of data transmission across the interconnected expanse of IoT devices and platforms, especially when unanticipated protocol translation systems and new devices are integrated within the networks. As these relays facilitate data transmission across different network layers and protocols, they inherently increase the system's attack surface, presenting potential vulnerabilities for exploitation that must be addressed from the beginning [43,44].

Implementing security measures can help in maintaining secure communications involving IoT relays. They help ensure safe and reliable transmission of data across diverse IoT ecosystems. This not only protects the network from potential threats, but also builds trust among users and stakeholders, fostering the growth and development of secure, interconnected IoT applications. Security measures like the following must urgently be taken into consideration when implementing systems like this project's Relay [45,46]:

4.1.1. Vulnerabilities and Long-Term Patching

Communication relays, by their function, could be targeted by attackers seeking to intercept or manipulate data. These nodes become critical points of security, especially considering they are exposed two-fold, as they need to interact with two different networks. Therefore, deep attention with robust protection measures are necessary. Encryption protocols, such as TLS/SSL, are vital in securing data in transit, ensuring that data passing through the relay remains confidential and tamper proof. Nevertheless, one must not ignore up-and-coming quantum computing, which may be used to break classic cryptographic algorithms in a matter of seconds.

Fortunately, so-called Post-Quantum Cryptography (PQC) is being actively developed, and has already proven to be reliable. PQC algorithms provide protection against both classical and quantum attacks, and they can be implemented on classical, binary computers [47–50].

This is a vital requisite to guarantee long-term security and integrity within IoT networks, as these devices are expected to continue relying on classic computing CPUs for years to come, even when quantum computing starts to settle in other fields. However, it is mandatory for vendors, developers, and the like to ensure current IoT devices receive

future firmware updates, as failing to do so may result in significant vulnerable points within larger networks.

Keeping the Relay and its connected devices updated with the latest security patches is fundamental in protecting against known vulnerabilities. Automated update mechanisms can facilitate this process, ensuring that the system is resilient against emerging threats.

4.1.2. Compliance with Standards and Risk Mitigation

Complying with established security standards and frameworks, such as those outlined by the International Organization for Standardization (ISO), provides a structured approach to securing IoT ecosystems. These standards offer guidelines on best practices for IoT security and risk mitigation, from device manufacturing to data transmission and storage. Security strategies should be adaptive, capable of evolving with the changing threat landscape and technological advancements in the IoT and in any other field.

4.1.3. Authentication and IDPS

Rigorous authentication mechanisms are essential for verifying the identity of devices, and especially users interacting with the Relay. Implementing strong, multi-factor authentication can significantly reduce the risk of unauthorized access. Access control policies further ensure that devices and users have only the necessary permissions, following the principle of least privilege.

Deploying intrusion detection and prevention systems (IDPS) at strategic points within the network can help in identifying and mitigating potential security breaches in real time. These systems monitor network traffic for suspicious activities, providing an additional layer of security by alerting administrators to possible attacks. IDPS become important in devices like this Relay, as they expose various network interfaces connecting matching distinct networks.

4.2. Future-Proofing—Scalability

The pivotal role of open-source technologies is monumental in the advancement of truly interconnected systems, platforms, and ultimately societies. The primary barriers to the current amalgamation and seamless interoperability of IoT systems mainly arise from proprietary strategies adopted by certain manufacturers. These entities aim to dominate the ecosystem with their unique technologies and protocols. A shift towards a more transparent approach, with shared developments and requirements, could not only accelerate economic growth and exceed market expectations, but also bolster security measures through early detection and vulnerabilities resolution.

The open-source paradigm, exemplified by Home Assistant technology, invites an extensive community of developers and end users to contribute towards swift and coherent evolution. This collaborative approach promises to expedite innovation, facilitating the introduction of novel devices and software solutions, thus catalyzing essential real-time interoperability for the IoT's future.

The NB-IoT, with its low power demand, wide area coverage, thoughtful design, and strong carriers' backing, stands out as an enormously capable backbone for supporting the scalability of IoT solutions like the one presented in this article. The NB-IoT's deep coverage and support, along with its minimal energy consumption model, is particularly advantageous for scalable IoT ecosystems, requiring fewer resources for connectivity while maintaining robust performance.

The narrowband-IoT's capabilities extend to ensuring longer battery life for connected devices, which is a critical consideration for IoT scalability. By enabling devices to operate for years on a single battery charge, the NB-IoT reduces the need for frequent maintenance, further lowering the resources required for a scalable IoT solution. This efficiency is particularly beneficial for applications in smart metering, asset tracking, and environmental monitoring, where devices are often deployed in tough, hard-to-reach scenarios.

HA's lightweight, flexible architecture allows for easy, virtually-endless integrations with a wide array of devices and services, including those leveraging NB-IoT technology. This ease of scalability makes it an ideal platform for deploying and managing large-scale IoT applications. The synergy between HAs' versatility and the NB-IoT's efficacious connectivity paves the way for creating extensive, reliable IoT networks that can grow and evolve with little effort.

The combined approach of utilizing Home Assistants for device management and the NB-IoT as a universal means of connectivity exemplifies a solution that demands as few resources and particularities as possible. This leads to a robust, ubiquitous framework for IoT harmonization as we claimed in this article. This framework helps accelerate the deployment of scalable solutions without the burden of resource allocation, infrastructure development, or maintenance.

The coordination of a few well-founded technologies presents a forward-thinking approach to IoT development. We believe that these such approaches will become more common. These combinations not only champion scalability and interoperability for IoT systems, but they also significantly reduce the expertise and concreteness often required for creating and expanding use case-tailored IoT solutions.

The (near) future of IoT lies in the adoption of open, efficacious, and scalable solutions, promising a more interconnected, truly harmonious and seamless IoT realm.

Author Contributions: Conceptualization, A.S and E.S.; methodology and validation, E.S. and G.d.C.; hardware and software, E.S. and I.G.; laboratory work, formal analysis, resources, visualization, and data curation, E.S.; investigation, E.S. and I.G.; writing—original draft preparation, E.S.; writing—review and editing and supervision, A.S.; project administration and funding acquisition, A.S. and G.d.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially supported by the CHIST-ERA EU project "ABIDI: Context-aware and Veracious Big Data Analytics for Industrial IoT" (PCI2019-103762), the Spanish National project "OPERA: Optics Designs to Improve the Performance of Radiative Cooling Systems" (TED2021-132660B-I00), both funded by the Spanish Ministry of Science, Innovation and Universities (MICIN); the HORIZON EU project "MOBILITIES for EU: New Mobility Solutions for Climate Neutrality in EU Cities" (101139666), funded by the European Commission; and the project"IoTMadLab: *Laboratorio IoT de Madrid*", an emerging Smart Cities Laboratory created by Madrid's City Council and UPM.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. IoT Analytics State of IoT 2021: Number of Connected IoT Devices Growing 9% to 12.3 Billion Globally, Cellular IoT Now Surpassing 2 Billion. Available online: https://iot-analytics.com/number-connected-iot-devices/ (accessed on 8 April 2024).
2. del Campo, G.; Gomez, I.; Cañada, G.; Piovano, L.; Santamaria, A. Guidelines and Criteria for Selecting the Optimal Low-Power Wide-Area Network Technology. In *LPWAN Technologies for IoT and M2M Applications*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 281–305, ISBN 978-0-12-818880-4.
3. Al-Kashoash, H.A.A.; Kemp, A.H. Comparison of 6LoWPAN and LPWAN for the Internet of Things. *Aust. J. Electr. Electron. Eng.* **2016**, *13*, 268–274. [CrossRef]
4. Wu, P.; Cui, Y.; Wu, J.; Liu, J.; Metz, C. Transition from IPv4 to IPv6: A State-of-the-Art Survey. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 1407–1424. [CrossRef]
5. Hyun, J.; Li, J.; Kim, H.; Yoo, J.-H.; Hong, J.W.-K. IPv4 and IPv6 Performance Comparison in IPv6 LTE Network. In Proceedings of the 2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS), Busan, Republic of Korea, 19–21 August 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 145–150. [CrossRef]
6. Lencse, G.; Kadobayashi, Y. Comprehensive Survey of IPv6 Transition Technologies: A Subjective Classification for Security Analysis. *IEICE Trans. Commun.* **2019**, *E102.B*, 2021–2035. [CrossRef]

7. Jara, A.J.; Ladid, L.; Skarmeta, A. The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2013**, *4*, 97–118. [CrossRef]
8. Samad, F.; Abbasi, A.; Memon, Z.A.; Aziz, A.; Rahman, A. The Future of Internet: IPv6 Fulfilling the Routing Needs in Internet of Things. *Int. J. Future Gener. Commun. Netw.* **2018**, *11*, 13–22. [CrossRef]
9. Ziegler, S.; Crettaz, C.; Ladid, L.; Krco, S.; Pokric, B.; Skarmeta, A.F.; Jara, A.; Kastner, W.; Jung, M. IoT6—Moving to an IPv6-Based Future IoT. In *The Future Internet*; Galis, A., Gavras, A., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2013; Volume 7858, pp. 161–172, ISBN 978-3-642-38081-5.
10. Newman, D. Return On IoT: Dealing with the IoT Skills Gap. Available online: https://www.forbes.com/sites/danielnewman/2019/07/30/return-on-iot-dealing-with-the-iot-skills-gap/?sh=5f453ccb7091 (accessed on 8 April 2024).
11. Savolainen, T.; Soininen, J.; Silverajan, B. IPv6 Addressing Strategies for IoT. *IEEE Sens. J.* **2013**, *13*, 3511–3519. [CrossRef]
12. Triantafyllou, A.; Sarigiannidis, P.; Lagkas, T.D. Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 5349894. [CrossRef]
13. Saavedra, E.; Mascaraque, L.; Calderon, G.; del Campo, G.; Santamaria, A. The Smart Meter Challenge: Feasibility of Autonomous Indoor IoT Devices Depending on Its Energy Harvesting Source and IoT Wireless Technology. *Sensors* **2021**, *21*, 7433. [CrossRef] [PubMed]
14. Saavedra, E.; Mascaraque, L.; Calderon, G.; Del Campo, G.; Santamaria, A. A Universal Testbed for IoT Wireless Technologies: Abstracting Latency, Error Rate and Stability from the IoT Protocol and Hardware Platform. *Sensors* **2022**, *22*, 4159. [CrossRef] [PubMed]
15. Nabu Casa Home Assistant | Documentation. Available online: https://www.home-assistant.io/docs/ (accessed on 8 April 2024).
16. Cujilema Paguay, J.A.; Hidalgo Brito, G.A.; Hernandez Rojas, D.L.; Cartuche Calva, J.J. Secure Home Automation System Based on ESP-NOW Mesh Network, MQTT and Home Assistant Platform. *IEEE Lat. Am. Trans.* **2023**, *21*, 829–838. [CrossRef]
17. Da Silva Campos, B.; Rodrigues, J.J.P.C.; Mendes, L.D.P.; Nakamura, E.F.; Figueiredo, C.M.S. Design and Construction of Wireless Sensor Network Gateway with IPv4/IPv6 Support. In Proceedings of the 2011 IEEE International Conference on Communications (ICC), Kyoto, Japan, 5–9 June 2011; IEEE: Piscataway, NJ, USA, 2011; pp. 1–5. [CrossRef]
18. Arzo, S.T.; Zambotto, F.; Granelli, F.; Bassoli, R.; Devetsikiotis, M.; Fitzek, F.H.P. A Translator as Virtual Network Function for Network Level Interoperability of Different IoT Technologies. In Proceedings of the 2021 IEEE 7th International Conference on Network Softwarization (NetSoft), Tokyo, Japan, 28 June–2 July 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 416–422. [CrossRef]
19. Grosse, E.; Lakshman, Y.N. Network Processors Applied to IPv4/IPv6 Transition. *IEEE Netw.* **2003**, *17*, 35–39. [CrossRef]
20. Kitamura, H. A SOCKS-Based IPv4/IPv6 Gateway Mechanism. Available online: https://www.rfc-editor.org/rfc/pdfrfc/rfc3089.txt.pdf (accessed on 8 April 2024).
21. Ghumman, F.A. Effects of IPV4/IPv6 Transition Methods in IoT (Internet of Things): A Survey. *SSRN* **2019**. [CrossRef]
22. Pycom FiPy Specsheets. Available online: https://docs.pycom.io/gitbook/assets/specsheets/Pycom_002_Specsheets_FiPy_v2.pdf (accessed on 8 April 2024).
23. Pycom Pybytes 3. Available online: https://docs.pycom.io/pybytes/ (accessed on 8 April 2024).
24. 1NCE 1NCE | About. Available online: https://1nce.com/en-eu/about (accessed on 8 April 2024).
25. Jiménez Ruíz, L. Diseño de Implementación de Etapa de Comunicación Basada En 6LoWPAN Para Plataforma Modular de Redes de Sensores Inalámbricas. Bachelor's Thesis, Universidad Politécnica de Madrid, Madrid, Spain, 2016. Available online: https://oa.upm.es/43013/1/TFG_LUIS_JIMENEZ_RUIZ.pdf (accessed on 8 April 2024).
26. del Campo, G.; Calatrava, S.; Canada, G.; Olloqui, J.; Martinez, R.; Santamaria, A. IoT Solution for Energy Optimization in Industry 4.0: Issues of a Real-Life Implementation. In Proceedings of the 2018 Global Internet of Things Summit (GIoTS), Bilbao, Spain, 4–7 June 2018; pp. 1–6. [CrossRef]
27. Ayoub, W.; Samhat, A.E.; Nouvel, F.; Mroue, M.; Prevotet, J.-C. Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs Standards and Supported Mobility. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1561–1581. [CrossRef]
28. Beyene, Y.D.; Jantti, R.; Tirkkonen, O.; Ruttik, K.; Iraji, S.; Larmo, A.; Tirronen, T.; Torsner, A.J. NB-IoT Technology Overview and Experience from Cloud-RAN Implementation. *IEEE Wirel. Commun.* **2017**, *24*, 26–32. [CrossRef]
29. Deutsche Telekom IoT NB-IoT, LoRaWAN, Sigfox: An Up-to-Date Comparison. Available online: https://testhardware.iot.telekom.com/LoadDocument/3522258863259434205/NB-IoT,%20LoRaWAN,%20Sigfox%20-%20An%20Up-to-date%20Comparison.pdf (accessed on 8 April 2024).
30. Gbadamosi, S.A.; Hancke, G.P.; Abu-Mahfouz, A.M. Building Upon NB-IoT Networks: A Roadmap Towards 5G New Radio Networks. *IEEE Access* **2020**, *8*, 188641–188672. [CrossRef]
31. Ratasuk, R.; Vejlgaard, B.; Mangalvedhe, N.; Ghosh, A. NB-IoT System for M2M Communication. In Proceedings of the 2016 IEEE Wireless Communications and Networking Conference, Doha, Qatar, 3–6 April 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–5. [CrossRef]
32. Mroue, H.; Nasser, A.; Hamrioui, S.; Parrein, B.; Motta-Cruz, E.; Rouyer, G. MAC Layer-Based Evaluation of IoT Technologies: LoRa, SigFox and NB-IoT. In Proceedings of the 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM), Jounieh, Lebanon, 18–20 April 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–5. [CrossRef]
33. Salva-Garcia, P.; Alcaraz-Calero, J.M.; Wang, Q.; Bernabe, J.B.; Skarmeta, A. 5G NB-IoT: Efficient Network Traffic Filtering for Multitenant IoT Cellular Networks. *Secur. Commun. Netw.* **2018**, *2018*, 9291506. [CrossRef]

34. Sánchez Rosado, D. NB-IoT Tecnologías Celulares Narrow-Band: Análisis Práctico de Las Soluciones de Telefónica y Vodafone. Master's Thesis, Universidad Complutense de Madrid, Madrid, Spain, 2019. Available online: https://docta.ucm.es/rest/api/core/bitstreams/28c3c5e5-4159-472b-bf0d-a9f21e546009/content (accessed on 8 April 2024).
35. Jia, G.; Zhu, Y.; Li, Y.; Zhu, Z.; Zhou, L. Analysis of the Effect of the Reliability of the NB-Iot Network on the Intelligent System. *IEEE Access* **2019**, *7*, 112809–112820. [CrossRef]
36. Mangalvedhe, N.; Ratasuk, R.; Ghosh, A. NB-IoT Deployment Study for Low Power Wide Area Cellular IoT. In Proceedings of the 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Valencia, Spain, 4–8 September 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–6. [CrossRef]
37. Wikipedia Constrained Application Protocol. Available online: https://en.wikipedia.org/wiki/Constrained_Application_Protocol (accessed on 8 April 2024).
38. Wikipedia Representational State Transfer. Available online: https://en.wikipedia.org/wiki/REST (accessed on 8 April 2024).
39. Nabu Casa, Home Assistant Community Home Assistant | Repositories. Available online: https://github.com/orgs/home-assistant/repositories (accessed on 8 April 2024).
40. Del Campo, G.; Saavedra, E.; Piovano, L.; Luque, F.; Santamaria, A. Virtual Reality and Internet of Things Based Digital Twin for Smart City Cross-Domain Interoperability. *Appl. Sci.* **2024**, *14*, 2747. [CrossRef]
41. Flask | Documentation. Available online: https://flask.palletsprojects.com/en/3.0.x/ (accessed on 8 April 2024).
42. CoAPython3. Available online: https://github.com/Tanganelli/CoAPthon3 (accessed on 8 April 2024).
43. Lencse, G.; Kadobayashi, Y. Methodology for the Identification of Potential Security Issues of Different IPv6 Transition Technologies: Threat Analysis of DNS64 and Stateful NAT64. *Comput. Secur.* **2018**, *77*, 397–411. [CrossRef]
44. Sabir, M.R.; Fahiem, M.A.; Mian, M.S. An Overview of IPv4 to IPv6 Transition and Security Issues. In Proceedings of the 2009 WRI International Conference on Communications and Mobile Computing, Kunming, China, 6–8 January 2009; IEEE: Piscataway, NJ, USA, 2009; pp. 636–639. [CrossRef]
45. Poole, O. *Network Security: A Practical Guide*; Computer Weekly Professional Series; Butterworth-Heinemann: Oxford, UK, 2003; ISBN 978-0-7506-5033-5.
46. Whitman, M.E.; Mattord, H.J.; Mackey, D.; Green, A. *Guide to Network Security*; Course Technology/Cengage Learning: Boston, MA, USA, 2013; ISBN 978-0-8400-2422-0.
47. Alagic, G.; Alperin-Sheriff, J.; Apon, D.; Cooper, D.; Dang, Q.; Liu, Y.-K.; Miller, C.; Moody, D.; Peralta, R.; Perlner, R.; et al. *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2019; p. NIST IR 8240.
48. Chen, L.; Jordan, S.; Liu, Y.-K.; Moody, D.; Peralta, R.; Perlner, R.; Smith-Tone, D. *Report on Post-Quantum Cryptography*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2016; p. NIST IR 8105.
49. Kumar, M.; Pattnaik, P. Post Quantum Cryptography(PQC)—An Overview: (Invited Paper). In Proceedings of the 2020 IEEE High Performance Extreme Computing Conference (HPEC), Waltham, MA, USA, 22–24 September 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–9. [CrossRef]
50. Song, F. A Note on Quantum Security for Post-Quantum Cryptography. In *Post-Quantum Cryptography*; Mosca, M., Ed.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2014; Volume 8772, pp. 246–265, ISBN 978-3-319-11658-7.