Rural Environmental Monitoring via ultra wide-ARea networKs And distriButed federated LEarning

Secure and trustworthy ML-based rural IoT platform architecture

Document Type	Deliverable
Document Number	D1.1
Primary Author	UPV
Dissemination Level	PU
Project Acronym	REMARKABLE
Project Title	Rural Environmental Monitoring via ultra wide-ARea networKs And distriButed federated LEarning
Grant Agreement Number	101086387
Project Website	https://remarkable.ulusofona.pt/
Project Coordinator	PDM
Version	2.0 | Final

REMARKABLE received funding from the European Research Executive Agency (REA) under grant agreement No 101086387 under the European Union's HORIZON Unit Grant research and innovation programme.

Authoring & Approval

Authors of the document

Name/Beneficiary	Position/Title	Date
Paolo Calciati / PDM	Project coordinator	01-06-2024
Pietro Manzoni / UPV	Professor	14-06-2024
Slavisa Tomic / ULHT	Professor	19-06-2024
Dejan Vukobratovic / UNS-FTN	Professor	28-06-2024
Srdjan Krco / DNET	Managing Director	19-06-2024

Reviewers internal to the project

Name/Beneficiary	Position/Title	Date
Yakubu Tsado / MMU	Researcher	27-06-2024
Paolo Calciati / PDM	Project coordinator	29-06-2024

Approved for submission to the REA by - representatives of beneficiaries involved in the project

Name/Beneficiary	Position/Title	Date
Luis Miguel Campos	Project coordinator	30-06-2024

Rejected by - representatives of beneficiaries involved in the project

Name/Beneficiary	Position/Title	Date

Document History

Version	Date	Status	Author	Justification
0.1	14/06/2024	Draft	Pietro Manzoni	First draft
0.2	19/06/2024	Draft	Slavisa Tomic	First draft update
0.3	24/06/2024	Draft	Slavisa Tomic	First complete draft
0.4	25/06/2024	Draft	Pietro Manzoni	Added minor corrections
1.0	28/06/2024	Draft	Dejan Vukobratovic	Update on the first draft
1.1	28/06/2024	Draft	Srdjan Krco	Update on the first draft
2.0	29/06/2024	Final	Paolo Calciati	Final version

Abstract

The main objective of REMARKABLE's WP1 is to design a secure and trustworthy Internet of things (IoT) platform for rural applications. To this end, the paramount attention will be given to device compatibility, energy efficiency, scalability, availability, security and flexibility challenges, by resorting to decentralised data-based methods, designing light-weight machine learning (ML) algorithms and deploying them at embedded edge IoT platforms. Moreover, device security and localisation will be targeted for edge ML methods, while data collected for ML training will be exploited for developing digital twin IoT platform models in parallel. Finally, the designed platform will be integrated with secure wide-area data analytics platform developed in WP3.

Therefore, this document describes the proposed secure and trustworthy ML-based IoT platform architecture. It defines the key requirements for the IoT platform and IoT devices, it identifies gaps in existing solutions, with regards to interoperability, scalability, security, energy efficiency and trustworthiness, and it provides implementation guidelines and summarizes the proposed architectural layout.

Table of Contents

List of Tables

List of Figures

1. Introduction

This document presents an extensive approach for the development of a secure and trustworthy machine learning (ML)-based Internet of things (IoT) platform particularly designed for rural applications. It proposes a robust architecture that ensures scalability, flexibility, energy efficiency, and enhanced security by addressing the essential requirements and identifying gaps in existing solutions. The envisioned architecture is tailored to surpass the unique challenges in rural settings, such as limited connectivity, power constraints, and the need for affordable, durable technology. It uses energy-efficient decentralised data-based methods, where light-weight ML algorithms are designed and deployed at embedded edge IoT platforms. Moreover, it foresees development of edge ML methods that target the device security and localisation, while at the same time, data collected for ML training will be used to develop digital twin IoT platform models. Lastly, the designed platform will be integrated with secure wide-area data analytics platform developed in WP3.

After providing an overall summary of the REMARKABLE project in the following section, the document elaborates on the proposed architectural layout for ML-based rural IoT platform design. It starts by defining the main requirements for IoT platform and identifying gaps in the existing commercial solutions. Based on these stipulations, the document then provides implementation guidelines and proposes a concrete architectural layout that accommodates and responds to all previously identified requirements and challenges. A summary of the main findings and conclusions is then provided, together with a comprehensive list of the published papers and the secondment experiences that played a vital role in shaping the overall proposed architecture.

1.1. Predefined Goals

The design of a secure and trustworthy IoT platform for rural applications, ensuring compatibility, scalability, flexibility, energy efficiency, and enhanced security, is the key component of the REMARKABLE's task 1.1 in the work package 1 (Grant Agreement, Description of the action, WP1, T1.1 [1]). This task is thus expected to result in an architectural layout for ML-based rural IoT platform design and the current document attests its value.

1.2. Applicable Reference Material

[1] Grant Agreement Number: 101086387 — REMARKABLE — HORIZON-MSCA-2021-SE-01.

[2] REMARKABLE Deliverable 6.3 - First Progress Report, available at: https://remarkable.ulusofona.pt/wp-content/uploads/sites/321/2023/08/REMARKABLE-D6.3-First-Progress-Report.pdf

[3] Minutes of the REMARKABLE Monthly Plenary Meetings – brainstorming sessions and discussions between partners.

1.3. List of Acronyms

Acronym	Definition
AI	Artificial Intelligence
CN	Communications and Networking

FL	Federated Learning
HAP	High-altitude Platform
IoT	Internet of Things
ICT	Information and Communication Technologies
LoRa	Long Range
ML	Machine Learning
NB	Narrow Band
LEO	Low-Earth Orbit
LoRaWAN	Long Range Wide Area Network
LP-WAN	Low-power Wide-area Network
LR-UWAN	Low-power Ultra-wide-area Network
LR-PAN	Low-rate Personal Area Network
NSS	Networked Sensing Systems
TinyML	A kind of embedded ML
UAV	Unmanned Aerial Vehicle
UC	Use Case

Table 1. List of acronyms.

2. Project Introduction

2.1. The REMARKABLE project

Internet of Things (IoT) technology combined with complementary support for data analytics is the cornerstone of today's digital transformation. The societal and economic impact of IoT/machine learning (ML) systems in urban and suburban areas significantly outpaces the one in rural areas due to a limited reach of connectivity infrastructure. IoT technologies have a huge potential for improving the economy and quality of life in rural areas, both in developed and developing countries. For instance, about 30.6% of the EU population lives in rural areas, which cover over 83% of the total EU area. Nonetheless, the average GDP per capita in rural EU areas is only 75% of the EU average [5]. Moreover, even though mobile networks cover more than 99% of the population in some European countries (such as the UK), they cover only about 79% of their landmass, thus leaving more than 20% of deep rural country areas without signal coverage [6]. To reverse further widening of the urban-rural gap, one needs to bring efficient and affordable IoT/ML solutions to deep rural areas, reaching out to applications and use cases ranging from wildlife management, rural tourism, livestock monitoring, water and air pollution control, and others.

REMARKABLE is an interdisciplinary project comprising experts from computer science, communication engineering, life sciences, environment and management. These experts come from diverse organisations in the UK, Europe and Africa. The project's vision is to bring IoT/ML systems a step closer to seamless, energy efficient and secure deployment targeting use cases in deep rural areas. This will be done by identifying main gaps in connectivity and affordable data analytics and through interleaved research, development and validation in a real-world setting. The project is centred on an IoT/ML-based technological platform that will be adapted and demonstrated in the context of use cases applied in environmental monitoring, management, and conservation.

In short, the REMARKABLE project emphasises a necessity of bringing rural areas into the reach of IoT/ML technologies. Its goal is to facilitate a reduction of urban-rural gap which is currently increasing. Making advanced information and communication technologies (ICT) such as IoT/ML systems a rural commodity will play a crucial role in reversing the rural depopulation trends due to an expanded range of economic opportunities through empowering and modernising traditional rural ecosystems. The added value of deploying IoT/ML in deep rural areas is in reaching out to new streams of data sources that could prove invaluable in tackling and better understanding the growing environmental concerns, ranging from local and regional (such as pollution monitoring) to global ones (such as climate change).

REMARKABLE considers several objectives in terms of research and innovation that will also have a large environmental and societal impact, summarised in Table 2.

	Objective	Outcome	WP-M	Deliverable	Respons. Partner
Research and Innovation Objectives	Secure and Trustworthy Sensing, Localisation and Digital Twins	Design of robust, secure, trustworthy, and traceable IoT platform suitable for deep rural applications	M44	D.1.1-D.1.4	ULHT
	Connecting the Unconnected – Ultra Wide-Area IoT Networks	Provide a solution for connectivity of IoT devices deployed in deep rural areas beyond the reach of current wireless cellular network infrastructure	M44	D.2.1-D.2.4	UNS-FTN
	Secure and Frugal Distributed Data Analytics for Rural IoT	Develop a novel data analytics platform based on privacy-preserving distributed ML methods that are frugal secure and scalable	M44	D.3.1-D.3.4	MMU
	Demonstration, Validation and Assessment	Demonstrate, validate, and assess developed solutions in use cases in real-life conditions, across European and African countries	M48	D.4.1-D.4.4	UA
Environmental and Societal Impact	Health and vitality monitoring of livestock in real-time	Enable quick animal treatment and prevent spreading illness, increase food production, track animals, identify grazing patterns, prevent desertification			
	Wildlife monitoring	Support tracking of endangered animals, reduce their poaching, improve tourist experiences in wildlife parks and reservations			
	Soil and agronomic management	Support automated irrigation and increase all-season production of food products			
	River pollution and air quality monitoring	Prevent health risk to humans, protect aquatic ecosystems from collapse and prevent the proliferation of phytoplankton			

Table 2. Summary of REMARKABLE project objectives.

2.2. Project key messages

REMARKABLE offers at least four main high-level messages that are foreseen for the principal findings produced by the projects, which are focused on the following concepts:

The REMARKABLE project is centred on developing an IoT/ML-based technological platform that will be adapted and demonstrated in the context of use cases applied to environmental monitoring, management, and conservation.

REMARKABLE uses and assesses innovative methodologies based on statistical data processing and decentralised federated learning methods specifically designed for different use case implementations and demonstrations.

The REMARKABLE project places a specific focus on rural environments and, in particular, on the African continent due to the huge potential of the number of IoT applications in Africa and the lack of traditional connectivity options.

REMARKABLE strives at developing various added-value services ranging from wildlife management, rural tourism, livestock monitoring, water and air pollution control and others.

2.3. Keywords

Distributed federated learning, Internet of Things, Rural environmental monitoring, Statistical data processing, Ultra-wide area networks.

3. The Remarkable proposed IoT platform architecture

This report outlines the proposal for a secure and trustworthy machine learning (ML)-based rural IoT platform architecture. It highlights the requirements, gaps in existing solutions, implementation guidelines, and the proposed architectural layout. The primary goal is to design an IoT platform that addresses security, scalability, flexibility, and energy efficiency challenges for rural applications.

3.1. Requirements for IoT Platform

Task 1.1 aims to define requirements for IoT devices deployed in rural use cases, identify gaps in existing commercial solutions regarding security and trustworthiness, and propose a novel secure and trustworthy IoT platform architecture using light-weight ML methods for device security, anomaly detection and localization.

In Deliverable 6.3, the main IoT platform requirements for IoT devices deployed in rural use cases were identified [2] as the following.

- The developed platform must be constantly available and highly scalable: Platform's constant availability (with minimal downtime) is crucial for most stakeholders that should always be able to access and benefit from the platform. Moreover, the platform should be scalable in the sense that one can add more devices and/or payloads from existing devices that automatically scale with every device/payload.
- Substantial consideration must be given to flexibility, resilience and security of the developed platform: Network evolution, reflected in the augmented levels of connectivity and automation, poses several challenges that need to be addressed, together with the growing dependence on poorly inter-operable proprietary technologies that may pose risk to people and surrounding environment. We foresee that platform's versatility could be maximized by unmanned aerial vehicle (UAV) assistance in many rural use cases.
- Secure connectivity extension is crucial for the developed platform: The platform should enable connecting currently unconnected remote rural areas in a reliable and sustainable manner. This could be achieved by designing a solution for ultra-wide area IoT networks, by possibly considering hardware improvements at both the IoT device and the network side, exploiting High-Altitude Platforms (HAPs), Low Earth orbit (LEO) satellites, as well as using UAVs to provide aerial data links beyond the coverage edges.
- The developed platform must be energy-efficient: The platform will aggregate enormous collection of heterogeneous data coming from multiple IoT sensors. It is therefore paramount to extract relevant features from the (unstructured) data and enable the platform to learn from it (and adapt according to it) in a frugal (in the sense of resource and data requirements) manner.

3.2. Gaps in Existing Commercial Solutions

Current commercial solutions for IoT platforms that can be used in rural areas, like Ubidots[1], ThingsBoard[2] or ThingSpeak[3] have several notable gaps that need addressing to ensure secure and trustworthy operation. One significant issue is the reliance on proprietary protocols, which hinders interoperability between different devices and systems. Promoting open standards and protocols, such as Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP), is essential to ensure seamless compatibility and communication across diverse IoT devices. These open standards facilitate easier integration, reduce vendor lock-in, and enhance IoT systems' overall flexibility and scalability.

Scalability challenges are another critical gap in existing solutions. Many current platforms struggle to efficiently handle the growing number of IoT devices and the vast amounts of data they generate. However, the implementation of cloud-native technologies and edge computing can effectively distribute the computational load and reduce latency, thereby improving the system's ability to scale dynamically. These technologies, with their ability to leverage microservices and containerization, allow for more flexible and resilient deployments. Edge computing, on the other hand, processes data closer to where it is generated, reducing the need for constant data transmission to central servers, thus reducing latency.

Energy (in)efficiency is a prevalent issue in many commercial IoT platforms, particularly those deployed in rural areas where power resources may be limited. However, the design of energy-efficient algorithms is a crucial step towards prolonging the operational lifespan of IoT devices and reducing overall power consumption. The use of low-power communication technologies, such as Long Range Wide Area Network (LoRaWAN) and Narrowband IoT (NB-IoT), can significantly enhance energy efficiency. These technologies are designed to consume minimal power while maintaining robust communication capabilities over long distances, making them ideal for rural IoT deployments.

The limited security features of current IoT platforms pose significant risks, as IoT devices are often deployed in vulnerable and remote locations. Incorporating multi-layered security approaches is essential to protect data and devices from potential threats. This goal requires implementing secure boot mechanisms to ensure that devices only run trusted software, enabling over-the-air firmware updates to patch vulnerabilities quickly, and utilizing robust authentication methods to prevent unauthorized access. Additionally, anomaly detection mechanisms powered by machine learning can help identify and mitigate security breaches in real time by monitoring device behaviour and detecting deviations from normal patterns.

In summary, to address the gaps in existing commercial IoT solutions, it is imperative to adopt open standards and protocols, leverage cloud-native and edge computing technologies for scalability, design energy-efficient algorithms using low-power communication technologies, and implement comprehensive, multi-layered security measures. These steps will enhance IoT platforms'

[1] https://ubidots.com/
[2] https://thingsboard.io/
[3] https://thingspeak.com/

compatibility, scalability, energy efficiency, and security, making them more suitable for deployment in rural areas.

3.3. Implementation Guidelines

We consider that a cloud-native architecture with microservices should be implemented to achieve scalability and availability. This approach allows for dynamic scaling and high availability by decomposing applications into smaller, independent services that can be developed, deployed, and scaled individually. Container orchestration tools like Kubernetes are essential for managing service deployment across multiple nodes, ensuring efficient resource utilization, automatic scaling, load balancing, and self-healing capabilities to maintain service continuity.

Flexibility and resilience can be further enhanced by developing modular hardware and software components. These components should be designed to be easily customizable or replaceable, allowing for quick updates and adaptations to changing requirements without disrupting the overall system. For instance, if a new feature is required, a new microservice can be developed and added to the system without affecting the existing services. Implementing redundant network paths and data storage is crucial for handling network outages and data corruption. This redundancy ensures continuous availability and data integrity, providing a seamless user experience even during partial system failures.

Leveraging energy-efficient communication protocols such as LoRaWAN and NB-IoT is vital for energy efficiency. These protocols are designed to provide long-range communication with low power consumption, making them ideal for IoT applications and devices. Optimizing machine learning (ML) algorithms to run on low-power devices using frameworks like TensorFlow Lite or TinyML can significantly reduce energy consumption while maintaining high performance. These optimizations allow for intelligent processing at the edge, minimizing the need for constant data transmission to the cloud and conserving energy.

Connectivity can be ensured using various innovative technologies. Unmanned Aerial Vehicles (UAVs) can be deployed to provide Internet access in remote or disaster-stricken areas, creating a temporary but reliable communication network. Mesh networks and Delay Tolerant Networks (DTNs) offer robust solutions for continuous connectivity, especially in environments where traditional network infrastructure is unavailable or unreliable. Integrating High-Altitude Platforms (HAPs) and Low Earth Orbit (LEO) satellites can enhance connectivity by providing wide-area coverage and low-latency communication links, ensuring uninterrupted access to critical services and information.

To enhance security and trustworthiness, implementing end-to-end encryption for data in transit and at rest is imperative. This ensures that data remains confidential and protected from unauthorized access throughout its lifecycle. Hardware-based security modules, such as Trusted Platform Modules (TPMs), provide additional layers of security by enabling secure boot processes and protecting sensitive data through hardware encryption. Furthermore, considering the use of blockchain technology can enhance data integrity and transparency. Blockchain's decentralized and immutable ledger system ensures that data remains tamper-proof and verifiable, fostering trust and accountability in the system. These measures, combined with regular security audits and updates, can effectively protect the system from potential security threats.

Ultimately, a holistic approach that combines cloud-native architecture, modular and redundant components, energy-efficient protocols, innovative connectivity solutions, and robust security measures is essential for creating a scalable, available, flexible, resilient, energy-efficient, and secure system. These strategies collectively ensure optimal performance, reliability, and trustworthiness in various operational scenarios.

3.4. Architectural Layout

The proposed architectural layout includes edge devices equipped with sensors and actuators embedded with TinyML models for local, on-device processing. These edge devices will also feature communication modules like LoRaWAN and NB-IoT to ensure energy-efficient and long-range connectivity. Security modules, including Trusted Platform Modules (TPM) and secure boot mechanisms, will be integrated to safeguard device integrity and data security from the collection point.

The proposed connectivity infrastructure is unique in its reliance on Unmanned Aerial Vehicles (UAVs). These UAVs provide dynamic and mobile connectivity, particularly in remote or temporary deployment scenarios. Additionally, mesh and Delay Tolerant Networks (DTNs) are implemented to enable robust and resilient local communication, ensuring data transmission continuity even in the face of network disruptions.

The introduction of UAVs or HAPs and LEO satellites creates more dynamic connectivity topology compared to using only single-hop low power wide area networks (LP WANs) such as LoRaWAN or NB-IoT. This fact calls for more frequent use of relaying in IoT connectivity, either using custom-designed protocols in the initial stages until the relaying is adopted in existing standards. We note that the first steps of introducing relaying to LP WANs is currently an ongoing process both in LoRa Alliance for LoRaWAN relaying and in 3GPP for the so called sidelink relaying.

Edge gateways are a critical component in the proposed architecture. They handle data aggregation and preprocessing tasks and provide local storage to manage data bursts and ensure low-latency access to recent data. Lightweight machine learning inference capabilities are embedded within these gateways, enabling real-time decision-making and actions based on the pre-processed data. Connectivity management, including multi-path communication strategies, is implemented at the gateway level to optimize network usage and reliability.

The cloud backend will serve as the central hub for more advanced operations. It will provide centralized data storage, ensuring that all collected data is securely stored and easily accessible for further analysis. Advanced machine learning training model and deployment will occur in the cloud, leveraging its computational power to develop sophisticated models that can be periodically updated and deployed back to edge devices and gateways. The cloud backend will also host a blockchain ledger to ensure data integrity, providing an immutable record of all transactions and data exchanges, thus enhancing trust and transparency within the system.

A hybrid cloud-edge approach will be adopted to enhance system performance and reliability, allowing for seamless integration and coordination between the edge and cloud components. This will enable dynamic workload distribution, where computationally intensive tasks can be offloaded to the cloud while latency-sensitive and real-time tasks are processed at the edge.

Overall, this architectural layout aims to create a comprehensive, efficient, and secure system capable of supporting various applications and use cases. Integrating advanced connectivity solutions, robust security measures, and sophisticated data processing capabilities ensures that the system can adapt to varying operational demands while maintaining high performance and trustworthiness.

The envisioned architectural layout is illustrated in Figure 1. The first block corresponds to the IT node which is a byproduct of WP1. The node has both connectivity (WP2) and data analytics (WP3) capabilities, embedding TinyML models for relatively light on-device processing, as well as communication modules such as LoRaWAN and NB-IoT for low-range and energy-efficient communication. Moreover, to protect the node's integrity and data security, it is integrated with a couple of security ingredients, such as TPM and secure boot mechanisms. The connectivity infrastructure is a versatile module, enhanced with UAVs, HAPs and LEOs. It provides a robust and resilient local communication by mesh and DTNs, so that communication flow is assured even in the event of network disruptions. Data aggregation is performed by the edge gateways, which also carries out data pre-processing and provides local storage to manage data bursts and ensures low-latency access to fresh data. By embedding lightweight ML inference capabilities within the edge gateway, it handles real-time decision-making and actions like connectivity management to optimize network usage and reliability. For more advanced processing, a cloud backend is introduced. It provides centralized data storage and ensures that data are stored securely and easily accessible. Furthermore, the cloud with its computational power supports development of sophisticated models that can be periodically updated and deployed back to edge devices and gateways. The cloud backend comprises a blockchain ledger to ensure data integrity, providing an immutable record of all transactions and data exchanges, strengthening in this way trust and transparency within the system. Finally, the architecture embraces a hybrid cloud-edge approach to boost the system performance (e.g., by workload distribution) and reliability, enabling smooth integration and coordination between the edge and cloud components.

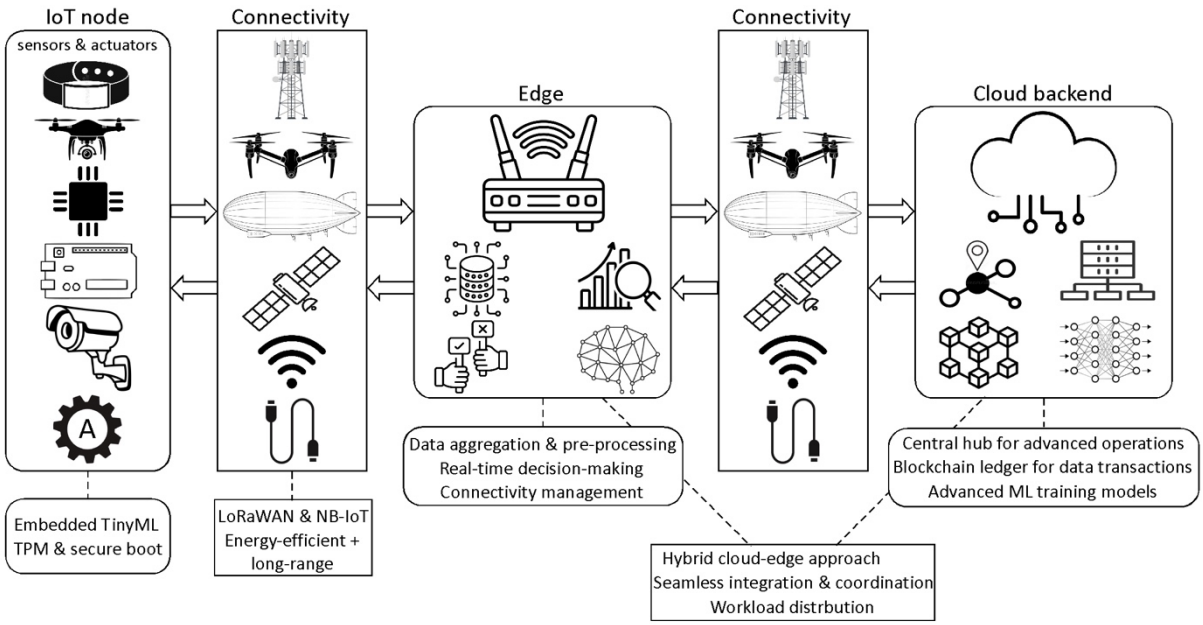

Figure 1. The proposed architectural layout for the secure and trustworthy ML-based rural IoT platform

3.5. Conclusion

This report presented a comprehensive approach to developing a secure and trustworthy ML-based IoT platform tailored explicitly for rural applications. It proposes a robust architecture that ensures scalability, flexibility, energy efficiency, and enhanced security by addressing the essential requirements and identifying gaps in existing solutions. The proposed architecture is designed to overcome the unique challenges in rural settings, such as limited connectivity, power constraints, and the need for affordable, durable technology.

Firstly, the architecture emphasizes scalability to accommodate the growth and variability in device deployments across vast rural areas. This is achieved through the adoption of a cloud-native architecture with microservices, enabling dynamic scaling of services and efficient resource management. Using container orchestration tools like Kubernetes ensures seamless service deployment and maintenance across distributed nodes, supporting an expanding network of IoT devices.

Flexibility is another critical aspect of the proposed solution. The modular design of hardware and software components allows for easy customization and replacement, catering to diverse agricultural practices and rural needs. This modularity also facilitates the integration of new technologies and updates without significant system overhauls, ensuring the platform remains adaptable to future advancements and changes in requirements.

Energy efficiency is paramount in rural applications where power sources are often limited or unreliable. The proposed architecture incorporates energy-efficient communication protocols such as LoRaWAN and NB-IoT, optimized for low power consumption and long-range transmission. Additionally, implementing TinyML models enables on-device processing, significantly reducing the need for constant data transmission to the cloud and conserving energy. Advanced ML algorithms are optimized for low-power devices using frameworks like TensorFlow Lite, ensuring intelligent local data processing with minimal energy expenditure.

Enhanced security is a cornerstone of the proposed platform, addressing the vulnerabilities inherent in IoT deployments. The architecture includes comprehensive security measures such as end-to-end encryption for data in transit and at rest, ensuring data confidentiality and integrity. Hardware-based security modules, including Trusted Platform Modules (TPMs) and secure boot mechanisms, protect the system from unauthorized access and tampering. Additionally, integrating blockchain technology provides an immutable ledger for data transactions, further enhancing data integrity and transparency.

Connectivity challenges in rural areas are being addressed through innovative solutions such as using UAVs for dynamic and mobile connectivity, mesh networks, and Delay Tolerant Networks (DTNs) for resilient local communication. These cutting-edge technologies ensure continuous connectivity, even in remote or infrastructure-limited locations, supporting reliable data transmission and system operation.

This report also highlights the importance of a hybrid cloud-edge approach, where computationally intensive tasks are offloaded to the cloud while latency-sensitive and real-time processing is handled at the edge. This balance optimizes performance, reduces latency, and ensures efficient use of resources, making the platform suitable for a wide range of rural applications.

In conclusion, this report proposed a comprehensive and forward-thinking architecture for an ML-based IoT platform designed for rural applications. By addressing scalability, flexibility, energy efficiency, and enhanced security, the proposed solution aims to create a resilient, efficient, and secure platform capable of meeting rural communities' unique challenges and needs. This architecture fills the gaps in existing solutions and paves the way for future innovations and improvements in rural IoT deployments.

3.6. Appendix

In this section, we provide a detailed account of the published papers and the secondment experiences that played a crucial role in shaping the overall proposed architecture. These contributions were instrumental in refining our approach and ensuring a comprehensive and robust design. The published papers offered valuable insights and advancements in the field, while the secondment provided practical, hands-on experience and facilitated collaboration with experts, leading to significant enhancements in our architectural framework.

Published Papers: [List of relevant published papers]

- M. A. Imran et al., "Exploring the Boundaries of Connected Systems: Communications for Hard-to-Reach Areas and Extreme Conditions," in Proceedings of the IEEE, doi: 10.1109/JPROC.2024.3402265.
- Peña-Haro, S., Arratia, B., Manzoni, P., and Cecilia, J. M.: Image-based System for Water Detection on Ephemeral Streams, EGU General Assembly 2024, Vienna, Austria, 14–19 Apr 2024, EGU24-9469, https://doi.org/10.5194/egusphere-egu24-9469, 2024.
- Benjamín Arratia, Erika Rosas, Carlos T. Calafate, Juan-Carlos Cano, José M. Cecilia, Pietro Manzoni, AlLoRa: Empowering environmental intelligence through an advanced LoRa-based IoT solution, Computer Communications, Volume 218, 2024, Pages 44-58, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2024.02.014.
- M. Altayeb, M. Zennaro, E. Pietrosemoli and P. Manzoni, "Optimizing the Performance of LoRaWAN Range Extenders in Sparse and Unconventional Contexts," 2023 IEEE Globecom Workshops (GC Wkshps), Kuala Lumpur, Malaysia, 2023, pp. 714-719, doi: 10.1109/GCWkshps58843.2023.10464980.
- L. Serena, P. Manzoni, M. Marzolla, G. D'Angelo, S. Ferretti, "Incentivizing Crowdsensing in IoT through Micropayments: a Simulation Study" 20th International Conference on Wireless and Mobile Computing, Networking and Communications, 21 - 23 October 2024 Paris, France (submitted)
- **S. Tomic** and **M. Beko**, “A Min-max Optimization-based Approach for Secure Localization in Wireless Networks,” IEEE Transactions on Vehicular Technology, vol. 73, no. 3, 4151—4161, March 2024. https://doi.org/10.1109/TVT.2023.3325063
- **S. Tomic** and **M. Beko**, “Trustworthy Target Localization via ADMM in the Presence of Malicious Nodes”, to appear in IEEE Transactions on Vehicular Technology, December 2023. https://doi.org/10.1109/TVT.2023.3346476
- R. Santos, **J. P. Matos-Carvalho**, **S. Tomic**, **M. Beko**, and S. D. Correia, “A Hybrid LSTM-based Neural Network for Satellite-less UAV Navigation”, 6th Conference on Cloud and Internet of Things (CIoT), Lisbon, Portugal, March 20-22, 2023. https://doi.org/10.1109/CIoT57267.2023.10084873

- R. Santos, N. Fachada, **J. P. Matos-Carvalho**, **S. Tomic**, and **M. Beko**, "AutoNAV: A Python package for simulating UAV navigation in Satellite-less Environments ", SoftwareX, vol. 27, pp. 1—12, September 2024. https://doi.org/10.1016/j.softx.2024.101782
- **S. Tomic**, **M. Beko**, D. Vukobratovic, **S. Krco**, and M. Costa, "Voting Scheme to Strengthen Localization Security in Randomly-deployed Wireless Networks", submitted to IEEE Transactions on Instrumentation and Measurement, June 2024.
- **J. Wubben**, **J. P. Matos-Carvalho**, **D. Pedro**, **S. Tomic**, and **C. T. Calafate**, "Empirical Evaluation of Multi UAV Coverage Path Planning for Aerial Surveying", in the 6th International Workshop on Wireless Sensors and Drones in Internet of Things (Wi-DroIT), Abu Dhabi, United Arab Emirates, April 29-May 1, 2024.
- R. Santos, **J. P. Matos-Carvalho**, **S. Tomic**, M. Beko, and **C. T. Calafate**, "Convolutional Neural Networks for autonomous UAV Navigation in GPS-denied Environments", submitted to 'Human-Centric Systems', 15th Doctoral Conference on Computing, Electrical and Industrial Systems (DoCEIS'24), Caparica, Portugal, July 3-5, 2024. https://doi.org/10.1007/978-3-031-63851-0_7
- S. D. Correia, **J. P. Matos-Carvalho**, and **S. Tomic**, "Quantization with Gate Disclosure for Embedded Artificial Intelligence Applied to Fall Detection", submitted to ACM 4th International Conference on Information Technology for Social Good (GoodIT 2024), Bremen, Germany, September 4-6, 2024.
- S. Sobot, M. Lukic, D. Bortnik, V. Nikic, B. Lima, M. Beko, D. Vukobratovic, "Two-Tier UAV-based Low Power Wide Area Networks: A Testbed and Experimentation Study," 6th Conference on Cloud and Internet of Things (CIoT), Lisbon (Portugal), March 2023.
- T. Devaja, S. Sobot, M. Petkovic, M. Beko, D. Vukobratovic, "Relay-Aided Slotted Aloha for UAV-Assisted Mixed UOWC-RF Systems," accepted, Int'l Symp. on Communication Systems, Networks and Digital Signal Processing - CSNDSP 2024, Rome, July 2024.

Secondments: [Details of secondments and contributions]

- **Jamie Wubben** (UPV) secondment at Beyond Vision, from October 1st, 2023, to November 30, 2023. Contributions of the secondment: "Orchestrating Multi-UAV Survey Missions: A Comprehensive solution for Path Planning, Collision Avoidance, and Ad-Hoc Networking"
- **Benjamin Arratia** (UPV) secondment at ICTP, from May 6th, 2024, to August 4th, 2024. Contributions of the secondment: "Transforming Environmental Monitoring: Integrating Machine Learning and IoT for Advanced Risk Detection
- **Marko Beko** (ULHT) secondment to DNET, from July 8th, 2023, to September 5th, 2023. Contributions of the secondment: "Studying existing commercial solutions and identifying IoT platform requirements for IoT devices deployed in rural applications".
- **Dajana Svrkota** (DNET) secondment to ULHT, from November 16th, 2023, to December 14th 2023. Contributions of the secondment: "Gap identification in existing commercial solutions for rural applications". The work done by DNET in the context of Horizon Europe COMMECT project focusing on digital transformation of rural regions was demonstrated, in particular the living lab deployment around Mrtva Tisa nature park, as an example of a combination of digital technologies (mobile renewable energy source, LoRaWAN and 4G communication, edgeML processing, video cameras, sensors, digital farming and environment monitoring platforms), as an input into preparation of this deliverable.

- **João Pedro Matos-Carvalho** (ULHT) secondment to UPV, from July 15th, 2023, to August 12th, 2023. Contributions of the secondment: "Applying light-weight ML solutions for IoT device localization in satellite-less environments".
- **Slavisa Tomic** (ULHT) secondment to DNET, from September 30th, 2023, to October 31st, 2023. Contributions of the secondment: "Identifying IoT platform requirements for IoT devices deployed in rural applications and developing frugal solutions for trustworthy IoT device localization"
- **Marko Beko** (ULHT) secondment to UNS-FTN, from November 30th, 2023, to December 30th, 2023. Contributions of the secondment: "Secure and trustworthy IoT device localization"
- **Christopher Stefan Erasmus** (STU) secondment to ULHT, from January 7th, 2024, to February 6th, 2024. Contributions of the secondment: "IoT LoRaWAN node development (a breadboard prototype) composed of a power supply, MCU, RFM95W LoRaWAN module, SD Card reader and Capacitive soil moisture sensor and a linear potentiometer dendrometer"
- **Slavisa Tomic** (ULHT) secondment to DNET, from March 23rd, 2024, to April 6th, 2024. Contributions of the secondment: "Strengthening localization/navigation security in adverse settings". Further, demonstration of a LLM-based decision support tool designed for farmers and rural regions was demonstrated, the challenges and potential ways forward discussed.
- **Mohammad Furqan Ali** (ULHT) secondment to STU, from May 1st, 2024, to June 30th, 2024. Contributions of the secondment: "A Trustworthy sensor network architecture of hybrid IoT/IoUT on terrestrial based UAVs and underwater bodies (AUVs)"
- **Srdjan Sobot** (UNS FTN) secondment to BEV, from March 09th, 2023, to March 23rd, 2023, and from July 18th, 2023, until August 01st, 2024. Contributions of the secondment: "Introduction of UAVs in IoT communication architecture"
- **Dejan Vukobratovic** (UNS FTN) secondment to BEV, from July 18th, 2023, until August 01st, 2024. Contributions of the secondment: "Design of novel IoT relaying architectures using UAVs"
- **Christopher Stefan Erasmus** (STU) secondment to ULHT, from June 17th, 2024, to September 06th, 2024. Contributions of the secondment: "Continuation of development and testing of the IoT LoRaWAN node"