POLITECNICO DI TORINO
Repository ISTITUZIONALE

A Framework for the Development of Sustainable Smart Services for the Countryside

*Original*
A Framework for the Development of Sustainable Smart Services for the Countryside / Blefari, F., D'Angelo, G., Ferretti, S., Furfaro, A., Giaccone, P., Marzolla, M., Pironti, F.A., Serena, L.. - In: COMPUTER. - ISSN 0018-9162. - ELETTRONICO. - (In corso di stampa). [10.1109/MC.2025.3592245]

*Availability:*
This version is available at: 11583/3002061 since: 2025-07-24T08:57:07Z

*Publisher:*
IEEE

*Published*
DOI:10.1109/MC.2025.3592245

*Terms of use:*

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

*Publisher copyright*
IEEE postprint/Author's Accepted Manuscript

©9999 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collecting works, for resale or lists, or reuse of any copyrighted component of this work in other works.

(Article begins on next page)

07 November 2026

# A Framework for the Development of Sustainable Smart Services for the Countryside

Francesco Blefari, *University of Calabria, Rende, 87036, Italy*
Gabriele D'Angelo, *University of Bologna, Bologna, 40126, Italy*
Stefano Ferretti, *University of Bologna, Bologna, 40126, Italy*
Angelo Furfaro, *University of Calabria, Rende, 87036, Italy*
Paolo Giaccone, *Politecnico di Torino, Torino, 10129, Italy*
Moreno Marzolla, *University of Bologna, Bologna, 40126, Italy*
Francesco Aurelio Pironti, *University of Calabria, Rende, 87036, Italy*
Luca Serena, *University of Bologna, Bologna, 40126, Italy*

*Abstract—The recent spread of smart city technologies has enabled the development of smart services and applications for citizens living in urban areas. However, deploying similar services sustainably in decentralized zones is challenging, primarily due to the lack of a stable communication infrastructure. Toward this goal, the use of secure and low-cost opportunistic networking technologies may play a key role in supporting the development of services based on cooperative (incentivized) communication models. We propose SUSY (SUstainable smart Services for the countrYside), a general architecture for the development of sustainable smart services. SUSY defines a set of high-level functionalities as building blocks for creating smart services in rural environments. Environmental sustainability is promoted through energy-efficient communication, decentralized processing, and incentive-driven ecological monitoring. We will refer to this vision of developing smart services in decentralized rural areas using the term "smart shires".*

***Index Terms:*** *Smart Environments, Opportunistic Computing, Blockchain*

In recent years, advances in the ICT domain have mainly been focused on "smart cities", with the goal of improving the services offered to citizens. All these services have been engineered on the assumption that they would be deployed in metropolitan areas. In the long-term, these efforts will have two relevant social effects: on one hand, they are likely to improve the quality of life of citizens. On the other hand, they will widen the differences among different areas of the same country or region. The problem is not just a matter of "digital divide": it is not possible to replicate smart cities services in rural areas and sparsely-populated regions, due both to the lack of the same infrastructures, but also because people living in metropolitan areas have different requirements and expectations than those living in the countryside [4].

With the term "smart shires", we refer to the set of digital and social solutions that allow the creation of innovative digital services in rural areas and improve their resilience, quality of life and economic prospects. We believe that the development of smart services for the countryside poses specific challenges that might be less prominent in other contexts. Rural areas are often poorly served by technological infrastructures that are given for granted in cities (high-speed network connections, energy distribution, utilities, and so on). A possible mitigation to digital resource scarcity is through sharing and adequate organization of data,

XXXX-XXX © 2025 IEEE
Digital Object Identifier 10.1109/XXX.0000.0000000

computation and communication protocols [18]. This has to be accomplished by integrating legacy access network infrastructures with alternative cooperative approaches, based on opportunistic and community-based mesh networks. Similarly, depending on the services to be provided, computation might be performed on cloud resources, on edge devices or through completely decentralized architectures. *Decentralized architectures* represent a paradigm shift from traditional centralized systems, where data authority, data storage, and computational tasks are distributed across multiple independent nodes within a network. This approach inherently enhances resilience, reduces single points of failure, and promotes autonomy among participating nodes. Distributed ledgers, decentralized file systems, fog computing and peer-to-peer networks are typical examples of decentralized system architectures, without having to rely on centralized "data silos", i.e., data stores that are controlled by a single entity. They can also be used in conjunction, in order to build more sophisticated services.

A key aspect of smart services is *cooperation*. Individuals should contribute storage, computing, and communication facilities, operate data relays or "smart" controllers that orchestrate part of the services for the benefit of the whole community.

To be technically and economically sustainable, sharing of network, computing and storage resources must be securely traced and rewarded. To this extent, blockchain-based techniques can provide accountability and incentives, since they offer proof of cooperation, which can be automatically awarded via smart contracts and the distribution of crypto tokens to be employed in the smart services ecosystem. These cooperative approaches not only address digital disparities but also support environmentally sustainable deployments by minimizing energy use and leveraging existing resources.

The goal of this paper is to define SUSY (SUstainable smart Services for the countrYside), a general architecture that allows the design and deployment of smart services in rural areas, overcoming infrastructure limitations through opportunistic networking and incentive-based cooperation. It includes a set of high-level functionalities that can be used as building blocks for developing smart services in rural environments. The SUSY architecture is descriptive rather than prescriptive: given the wide variety of available technologies (e.g., for smart sensors, microcontrollers, programming languages and software frameworks), we focus on functionality since implementation details are subject to non-functional requirements on a case-by-case basis. To illustrate the potential of our proposal, the paper discusses a set of real-world applications and explains how these are supported by the architecture.

Figure 1 illustrates the typical scenario where smart applications can be deployed. Rural or remote locations rely mostly on an opportunistic approach based on wireless communications, since wired broadband might not always be available, or too expensive; vehicles or pedestrians can act as "data mules" to collect data from various data sources (e.g., smart bins that can sense the environment and also their own status to alert the waste management service when they are full). Broadband access available at some homes may act as gateways to the Internet upon compensation to the respective operators.

## Smart Shires Applications Ecosystem

In this section, we discuss a few examples of applications that can be made possible by the SUSY architecture, based on use cases that we have been investigating in recent years.

### Trusted Data Mule

Trusted data mules introduce a decentralized approach to opportunistic networking, designed to address the challenge of data transmission in remote environments where traditional Internet access is unreliable or expensive. A data mule is a mobile physical entity (e.g., a vehicle) that collects data from devices it encounters during movement, stores it temporarily, and delivers it to designated destinations. Communication between offline devices and this vehicle typically happens via short-range wireless communication [5]. If not all devices can directly reach the road where vehicles travel, nodes in the area can form an overlay network to extend the communication range. Data are preferably stored using decentralized mechanisms (e.g., IPFS [1]), which helps ensure persistent availability by eliminating reliance on a single point of failure. A publish/subscribe-based announcement service allows recipients to discover and retrieve stored data by notifying them as soon as new content is available. Alternatively, retrieval can be performed using content identifiers, granting access without requiring a direct connection to the original sender. Contributions are incentivized using the secure cooperation layer, which ensures transparent reward distribution.

Smart data mules can be efficiently adopted also with individual human mobility. Health monitoring is a relevant use case. Consider the scenario of people

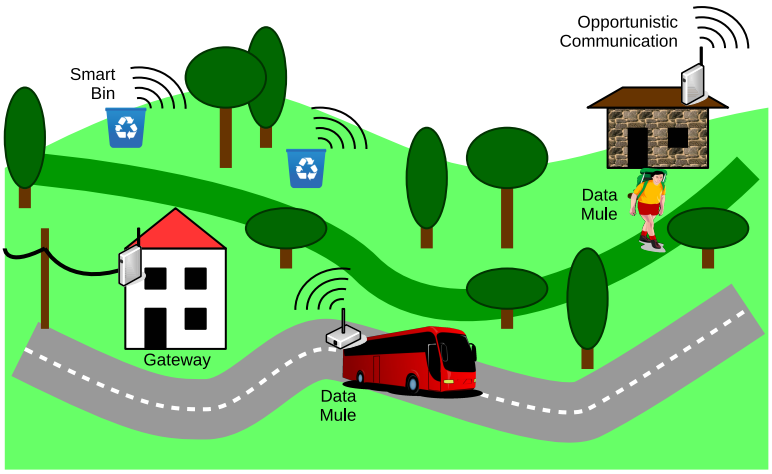



**FIGURE 1.** An example of smart services for the countryside.

living in rural areas without connectivity who, due to old age or known health conditions, require constant monitoring. To enable them to continue living in those areas, they may be equipped with environmental and wearable sensors.

In case of emergency, the wearable sensor system triggers a direct phone call to the nearest emergency department. In normal activity, collected data are stored, but they must be periodically transmitted to the central server of the public health system. In this case, sensitive data may require the adoption of trusted data mules that periodically visit him or pass nearby [20]. Edge computing allows for (preliminary) data processing at the patient's house. Proper authorization schemes are employed to understand who is eligible to treat which kind of data. Secure ad-hoc, short-range communication technologies are employed to transmit data. Blockchain mechanisms allow for secure tracing of all steps. People involved in the secure data transmission are rewarded with crypto-tokens that can be used in the area to pay for other smart shires enabled services. This mode of data collection minimizes infrastructure reliance and supports low-energy, sustainable data transport across rural landscapes.

## Incentive-based Environmental Monitoring

Another useful application is the collection of sensor data across remote environments, in particular where Internet connectivity is problematic. Examples are the collection of environmental data such as air quality, temperature, humidity, or pollutant levels in rural areas, forests, or agricultural zones [8], [12].

*Communication* can be handled using LoRaWAN [7] technology, which is well-suited for monitoring activities where traditional communication infrastructure is lacking. The adopted communication technology can transmit data over long distances with low power consumption, extending sensor battery life and reducing the effort for maintenance. Sensor data are collected by gateways, which can be either stationary, placed in optimally placed locations, or mobile, mounted on vehicles to enable opportunistic data collection, such as in the trusted data mule use case [13].

To stimulate *cooperation*, economic incentives are introduced to encourage individuals and organizations to participate in the data collection and transmission process. Smart contracts can automate the management of rewards by issuing micropayments to contributors, such as vehicle owners and service operators, based on predefined criteria like data volume or quality. To enable the trading of collected data, a *marketplace* can be integrated into the system where users subscribe to specific data streams of interest according to a publish-subscribe scheme. Alternatively, data could be stored on edge nodes, allowing for the collaborative training of machine learning models. This motivates the adoption of a federated learning setup, where models are trained locally on each device, and only aggregated updates are shared, minimizing the risk of sensitive data exposure.

Data from IoT sensors should be signed and encrypted to ensure *authenticity and confidentiality*, but these operations can be energy-intensive for low-power devices, making it necessary to find a balance between security and energy efficiency. Indeed, power consumption is a challenge for the development of

smart services, since most IoT sensors have to be powered by small solar panels or batteries. While blockchain ensures traceability, it must also protect privacy by avoiding the storage of sensitive information, such as the geographic location of identifiable users. Pseudoanonymity makes it hard to link transactions to real-world users, and limiting metadata exposure further reduces the risk of identity inference.

*Modeling and simulation* play a crucial role in the design phase by assessing the feasibility of the system to be implemented and identifying potential issues early in the process, e.g., evaluate the performance of delay-tolerant networks, the ability of blockchain to manage all required operations, and effectiveness of wireless communication. Multilevel modeling is well suited for analyzing complex IoT scenarios, as it allows different aspects of the system (e.g., blockchain activities, data transmission, and vehicle mobility) to be modeled independently, favoring code reusability and modular design [19].

### Smart Trails

In recent years, shifting tourism paradigms have led to the rise of a sustainable approach to countryside exploration. This form of "slow tourism" emphasizes the desire of individuals to explore at a leisurely pace, often by foot or through eco-friendly mobility options such as bikes.

In this framework, tourists may function as data mules, leveraging their smartphones to collect and transmit data for the smart shire. Services enabled by this infrastructure are strategically positioned along tourist trails and encompass a wide range of applications. Examples include monitoring terrain and air quality, deploying smart waste bins, enhancing services for mountain huts, offering exploration and proximity-based gaming experiences, and providing smart counters. These services create a comprehensive soft infrastructure that enriches the tourist experience while supporting environmental and community goals.

The communication technologies underpinning this ecosystem are those commonly integrated into modern smartphones, such as 5G, Bluetooth Low Energy (BLE), and Wi-Fi 7. These technologies facilitate the seamless operation of the data mule infrastructure, which is further reinforced by the cooperation layer, which ensures that participants are rewarded fairly and transparently [2]. This model supports green mobility and reduces carbon impact by replacing fixed sensor networks with human-carried devices.

By offering crypto-tokens as rewards, the system not only incentivizes participation but also strengthens the shire's economic ecosystem [16]. Tourists are encouraged to spend their tokens locally, creating a virtuous cycle that benefits both the visitors and the community. This approach represents a new model for sustainable tourism, where technology and ecological awareness create value for all involved parties. The *InDaMulC2C* framework [17] introduces direct client-to-client (C2C) communication by leveraging data mules and blockchain while still retaining the feature of client-server interaction. This framework can be employed as the communication backbone in a countryside scenario and supports two interaction modes:

- *Offline Interaction:* A single data mule carries the payload between two clients within the same geographical area, completing the exchange without server mediation.
- *Opportunistic Online Interaction:* Data mules upload payloads to a distributed file system when in connectivity zones, enabling proxies to facilitate the delivery.

For both modes, the protocol utilizes enhanced data structures, such as encrypted payloads and verification proofs, to ensure secure and reliable data transfer. These innovations reduce dependency on centralized servers, offering a cost-effective and resilient solution for communication in regions with poor connectivity

## SUSY architecture

Figure 2 shows the components of the SUSY architecture for smart shires applications. The architecture is loosely organized as a layered structure. The bottom layer implements the *communication service*, leveraging any standard communication medium and protocol. Wireless communications play a key role, since they enable data exchange among entities that might be mobile, or placed in remote locations. Communication may involve point-to-point data exchange between peers in direct contact, or more complex interactions. However, the SUSY architecture is agnostic with respect to the specific networking technologies being utilized.

The *network architecture* layer level sits on top of the communication layer, and is responsible for building and maintaining a virtual topology over the logical entities that are part of the application. A frequently used virtual topology is a mesh network that allows mobile entities to establish and maintain multi-hop routes. Another service that might be realized by the virtual topology management level is some form of Delay Tolerant Network (DTN), in which the nodes mobility is leveraged to move the data from one node to another, throughout the store-carry-forward paradigm. Indeed,

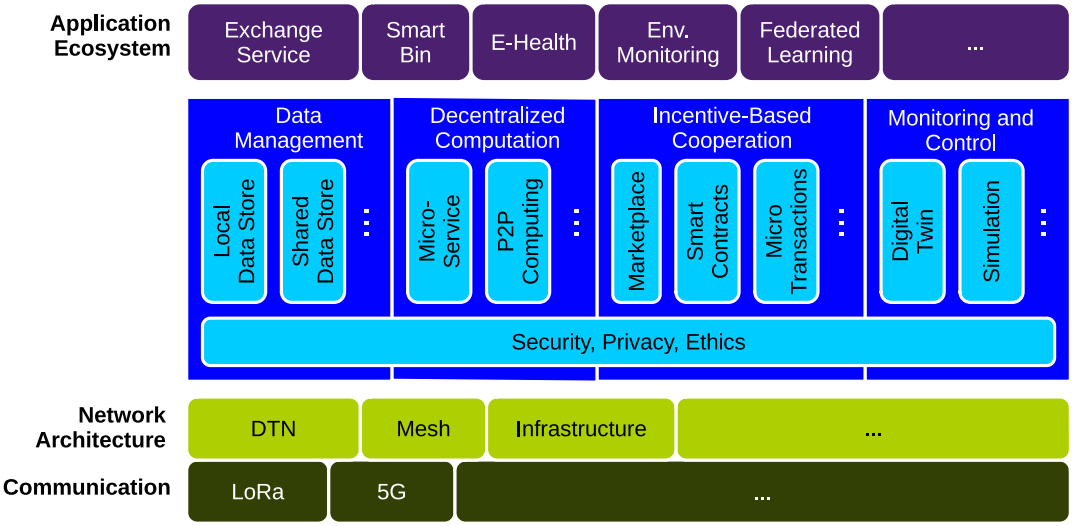



**FIGURE 2.** SUSY architecture.

in a rural scenario it is quite common that nodes remain isolated always or for extended periods of time, but the presence of mobile nodes visiting sporadically the area (e.g., agricultural vehicles/workers, tourists) enables a DTN approach.

The components that are specific for smart shires applications sit on top of the virtual topology management layer. They are grouped in four functional blocks:

- *Data management*, which provides services for storing and retrieving structured data and handling access control.
- *Decentralized computation*, which provides application-oriented computation services that might be carried out locally or remotely to realize micro-services that can be easily composed. This supports peer-to-peer computing scenarios.
- *Incentive-based cooperation*, which implements reward mechanisms to encourage participation, resource sharing and honest cooperation among the involved parties.
- *Monitoring and control*, which provide components for monitoring and managing the state of the communication resources, measure the performance, and react to changes in the environment to ensure the survivability of the application.

*Security, privacy and ethics* are cross-cutting concerns that impact all functional blocks and must be realized "by design" rather than by mere API calls.

There is no layered structure among the components above, because their concrete realization depends on implementation details such as the available hardware platforms, the software libraries or frameworks employed, and so on. Therefore, the architecture illustrated in Figure 2 is not a blueprint, but an inventory of functionalities that might be needed to build sustainable smart applications. Systems architects can choose which components are needed, how they are implemented, and how they interact according to the application requirements.

## Security, Trust and Ethics

As for any digital system that stores and performs elaboration on data belonging to citizens, or to other legal entities, security requirements play a critical role in ensuring that they are trustworthy. Taking care of such requirements from system's inception and then properly taking them into account since the early design stages favor the achievement of secure and reliable applications [14], [10]. Thus, the security requirements of the proposed architecture are pervasive to all the system components and they can be illustrated with reference to a set of basic properties that must be guaranteed in adherence to the principles of information security: *confidentiality*, *integrity* and *availability*. These properties are foundations for the trust in the smart shire architecture, and in the whole deployed system, by the final users. To guarantee these properties, suitable *authentication*, *authorization* and *auditing* mechanisms have to be put in place.

Confidentiality refers mainly to the management of information in the system architecture. The access

to user information is controlled by a specific Data Management module while data are protected in transit and at rest by means of appropriate encryption mechanisms. A central design principle of the architecture is to minimize the amount of unencrypted data that is transferred, processed and stored.

Integrity is the second basic property that must be provided by the system, and it refers to both the users' information and the architecture itself. For what concerns communications integrity, encryption protocols are again the mechanism to rely on. The situation is more complex for what concerns the data needed by the components to provide the desired services. The innovation proposed in SUSY relies on the usage of blockchain technologies. In fact, the immutability provided by the distributed ledger is a fundamental baseline for guaranteeing the required level of integrity and accountability, while preventing risks of single-point manipulation, typical of centralized solutions. In particular, a relevant part of the runtime logic of SUSY is implemented by smart contracts running on top of the blockchain. Finally, a smart shire requires the adoption of hardware components that are placed in public spaces. Being able to guarantee the physical security of these devices from tampering is a challenging task that needs to be addressed from both design and implementation viewpoints.

Attacks to the availability of the proposed architecture are possible and cannot be completely avoided. For example, Denial-of-Service (DoS) attacks may abuse some parts of the architecture for the sake of disrupting it. However, there are many mitigations that can be put in place. First of all, the distributed and sparse nature of the physical infrastructure has a dual effect: it makes it hard to avoid local attacks, but at the same time it avoids the presence of a single point of failure.

A promising target for attackers is the incentivization mechanism. A possible countermeasure is to minimize – by design – the possibility for the attackers to profit from the attacks. In other words, smart applications should avoid solutions that could be leveraged by attackers to profit from attacking it.

In cooperative scenarios where resources and services are shared, accountability (i.e., keeping track of who does what) is required to avoid that some parties abuse the system. However, accountability may clash with privacy, which is a fundamental right of every human being. This clash must be addressed through privacy-aware implementations, e.g., proper choice of the communication protocols. In situation where storing users' data can not be avoided, care must be taken to guarantee confidentiality not only from attackers, but also from malicious system administrators.

## Data Management Service

The Data Management module implements an access control mechanism designed to provide granular and secure data access management across personal and common data stores. The core of this system is an Access Control List (ACL) implemented through smart contracts, which enables fine-grained user-controlled data sharing and protection [3], [15].

The Data Store (DS) acts as a secure repository for storing application data. Data may come from the user directly, or produced by some application or services that have the authorization of generating data. The DS can be distributed across distributed nodes within the system. However, at the level of the single user, the DS acts as a centralized location to maintain control over his personal information, allowing to manage and update users' data efficiently.

The implementation of a DS can be achieved through various architectural approaches, ranging from centralized personal cloud storage services (e.g., Azure or Google Drive) to decentralized file storage systems like the InterPlanetary File System (IPFS) [1]. While centralized proprietary solutions typically offer ease of management and accessibility from an end-user perspective, decentralized data management architectures allow for data replication, being based on a peer-to-peer system organization, still relying on privacy through data encryption and users' pseudo-anonymity. Clearly enough, this kind of technology can also be used to create a private decentralized file systems that grant access to authorized users, only. Finally, all modifications to the DS can be tracked by recording updates in an associated distributed ledger technology, thereby ensuring data integrity and traceability.

Through SUSY functionalities, users can define and modify access permissions for their personal data stores. This means that users can specify granular access rights, including read, write, and partial data access for different entities. At any given time, the user retains the ability to add or remove other actors from the list of authorized users with access and writing privileges to his personal data. This can be achieved through a decentralized ACL implemented with smart contracts.

## Decentralized Computation Service

The need to enable the development of smart shires requires a sophisticated approach to the management

and distribution of computational resources. The decentralized computation service implements a flexible and scalable approach to distributed computation. At its core, the service adopts a microservice-based paradigm that virtualizes available resources (compute, storage, and network). This virtualization layer enables dynamic resource allocation and service composition, allowing the system to adapt to varying computational demands and environmental conditions. It also fosters peer-to-peer computation strategies, when needed.

SUSY relies on mobile device-edge continuum and fog computing, where end-user devices assume an active role in the computational ecosystem. This approach creates a spectrum of computational resources, extending from edge devices to fog nodes and cloud infrastructure. Containerization and orchestration technologies are required in order to cope with the heterogeneity of computation environments. Indeed, each containerized microservice can independently run in an isolated execution environment and be efficiently used and composed with other services through orchestration. For example, in a federated learning scenario, each component can operate within a container on each participating node, enabling secure model training while maintaining data locality.

## Incentive-based Cooperation Service

A critical aspect of successful decentralized systems is the implementation of effective incentive mechanisms for cooperation. Reward systems foster consistent and honest participation, maintain network stability, and fairly compensate contributors for their resources and efforts. These mechanisms become particularly relevant as they address the “free-rider” problem and motivate high-quality contributions to the shared model.

The Incentive-based Cooperation Service facilitates cooperation and incentivizes beneficial behaviors in SUSY. It incorporates a dynamic reputation system that adjusts based on node actions and task performance, influencing future SUSY task allocations and reward calculations. In addition, it implements a fair and transparent reward system based on node contributions and reputation.

Other incentive models beyond crypto-tokens have been investigated in the literature [9]. However, our framework prioritizes crypto-token as they offer decentralized governance and reduced vulnerability to centralized control.However, the incentive layer is designed to be adaptable: alternative mechanisms such as reputation scores, community recognition, or access to enhanced services can be used based on contextual needs and social preferences.

### Rewarding through Smart Contracts

The SUSY reward mechanism is based on a dedicated smart contract-based service, which automates the distribution of incentives based on predefined criteria, such as the quality of the contributed data, the amount of computational resources provided, and the cooperation by participating in an ad-hoc communication network or a DTN. All cooperating nodes receive rewards based on their contributions. In its internals, the smart contract tracks individual participant metrics including contribution scores and accumulated rewards. In SUSY, rewards are implemented as crypto-tokens that serve as assets to be used in the smart shire application ecosystem. This encourages local reinvestment of earned crypto-tokens, strengthening local, low-carbon economies.

### Verifiable Cooperation

Tied to the idea of using incentive mechanisms, there is the concept of verifiable cooperation, i.e., a mechanism in charge of validating collaborative behavior in decentralized systems. Once verified, these evidences of cooperative actions are recorded on the blockchain [11]. The specific verification mechanism can vary significantly depending on the type of cooperation involved. While some scenarios may require dedicated verifiers for proof generation, others might depend on certifying job completion through trusted execution environments, and yet others may rely on validation through dedicated sensors. An evaluation framework is needed to assess not only the quantity but also the quality of cooperative actions. This includes metrics such as task completion accuracy, response time and resource contribution effectiveness. Moreover, the more a node cooperates over time the higher the reward. The temporal aspect helps to prevent manipulation and ensures long-term network stability. The enforcement of temporal consistency specifically prevents malicious users from attempting to exploit the system through short-term fake cooperation to gain quick rewards.

## Monitoring and Control

The SUSY monitoring and control module is responsible for managing network resources in real time. In the considered scenario, the network is characterized by heterogeneity and temporal variability of the communication links, due to node mobility and variable communication conditions. This implies a very dynamic

network topology that should be properly exploited to transfer the data from a source to the desired destination/s. Monitoring tools retrieve in real time the state of the network topology, in terms of link connectivity, communication link performance (e.g., transmission rate, load) and node mobility. The monitoring data are fed in real time to a digital-twin of the network, defined through a time-evolving graph topology whose network resources, node connectivity, link rates and load are matched to the actual state of the real network. The actual state of the digital twin is cloned into a simulation model, which is adopted to experiment the effects of different control logics, in a speculative manner.

## Discussion and Conclusions

In this paper, we have introduced SUSY (SUstainable smart Services for the countrYside), a novel architecture specifically designed to address the challenges of implementing smart services in rural and sparsely populated areas. Thus, SUSY fosters the development and sustainability of smart shires. Unlike traditional smart city approaches, it acknowledges the fundamental differences in infrastructure, needs, and social contexts that exist in rural communities, offering an adaptable framework rather than attempting to re-use services implemented for smart cities.

We believe that rural areas require specifically designed smart services rather than adaptations of urban solutions, as they face distinct challenges including limited technological infrastructure and different user requirements. SUSY attempts to address digital resource scarcity through sharing mechanisms and proper organization of data, computation, and communication protocols. The architecture integrates legacy networks with alternative cooperative approaches, including opportunistic and community-based mesh networks, while implementing decentralized storage and computing models that eliminate dependence on centralized data silos, enhancing resilience and community ownership. To sustain these systems, SUSY incorporates blockchain-based accountability and reward mechanisms that provide incentives for community participation and resource sharing. The modular nature of the SUSY architecture enables seamless scaling by allowing components to be independently replicated or extended. As more devices or nodes are added, decentralized communication and computation models distribute the load effectively, ensuring the architecture remains responsive across large and heterogeneous rural regions.

The implementation of this architectural design can use different technologies that are currently available or under development. The interoperability of these components, although not strictly required, is certainly beneficial to foster the adoption of SUSY, since the possibility to easily swap components with functionally equivalent ones increases flexibility. Significant efforts are being made in inter-blockchain protocols that would address issues related to interoperability, standardization, and scalability. This would allow, for example, each shire to utilize its own ledger, which can be interoperable with others when necessary.

In our view, SUSY represents more than a technological solution; it embodies a socio-ethical vision for rural sustainability and development. Only by promoting the creation of smart services for these decentralized communities, we might try to slow or even reverse rural depopulation trends. By employing existing technologies in context-aware ways, we can create more inclusive technological futures that sustain rural communities rather than depleting them, while promoting low-impact, eco-conscious smart service models.

We are currently working to further validate the SUSY architecture, not only by means of prototypes for new case studies, but also ad-hoc modeling and simulation techniques that will enable a larger number of scenarios to be examined quickly. Specifically, multilevel modeling techniques proved to be well suited for the analysis of smart applications [6]. Moreover, while most of the existing work focused on functional aspects, we plan to address non-functional properties in more detail, such as privacy and security. The structure, mechanics and efficiency of financial incentives are of particular importance, since they are crucial for the wider adoption of smart services in rural areas.

## Acknowledgments

This work has been funded by the European Union - NextGenerationEU within the framework of PNRR Mission 4 - Component 2 - Investment 1.1 under the Italian Ministry of University and Research (MUR) programme “PRIN 2022” - grant number 2022N2NH42 - SmartShires - CUP: H53D23003570006.

## REFERENCES

1. InterPlanetary File System. https://docs.ipfs.tech/.
2. Mark C. Ballandies. To incentivize or not: Impact of blockchain-based cryptoeconomic tokens on human information sharing behavior. *IEEE Access*, 2022.
3. Fadi Barbàra, Mirko Zichichi, Stefano Ferretti, and Claudio Schifanella. DLT-based personal data access control with key-redistribution. In *International*

*Conference on Blockchain Computing and Applications (BCCA)*, 2023.

4. Jesús J. Cambra-Fierro and Lourdes Pérez. (Re)thinking smart in rural contexts: A multi-country study. *Growth and Change, Wiley*, 2022.
5. Jon Crowcroft, Eiko Yoneki, Pan Hui, and Tristan Henderson. Promoting tolerance for delay tolerant network research. *SIGCOMM Comput. Commun. Rev.*, 38(5):63–68, September 2008.
6. Gabriele D'Angelo, Stefano Ferretti, and Vittorio Ghini. Multi-level simulation of internet of things on smart territories. *Simulation Modelling Practice and Theory*, 73:3–21, 2017. Smart Cities and Internet of Things.
7. Ivan Fardin, Stefano Milani, Francesca Cuomo, and Ioannis Chatzigiannakis. Enabling edge computing over LoRaWAN: A device-gateway coordination protocol. In *ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, DIVANet, 2022.
8. Bogdan Cristian Florea and Dragos Daniel Taralunga. Autochain: An incentive-based blockchain system for air quality monitoring and emissions reduction. In *Proceedings of the 2023 6th International Conference on Blockchain Technology and Applications*, ICBTA '23, page 85–91, New York, NY, USA, 2024. Association for Computing Machinery.
9. Rong Han, Zheng Yan, Xueqin Liang, and Laurence T. Yang. How can incentive mechanisms and blockchain benefit with each other? a survey. *ACM Comput. Surv.*, 55(7), December 2022.
10. Chris Hankin. *ACM TechBrief: Smart Cities*. ACM, April 2022.
11. Yunhua He, Hong Li, Xiuzhen Cheng, Yan Liu, Chao Yang, and Limin Sun. A blockchain based truthful incentive mechanism for distributed p2p applications. *IEEE Access*, 6:27324–27335, 2018.
12. Cornelius Ihle, Dennis Trautwein, Moritz Schubotz, Norman Meuschke, and Bela Gipp. Incentive mechanisms in peer-to-peer networks — a systematic literature review. *ACM Comput. Surv.*, 55(14s), July 2023.
13. Peter Kietzmann, José Alamos, Dirk Kutscher, Thomas C. Schmidt, and Matthias Wählisch. Delay-tolerant icn and its application to lora. In *Proceedings of the 9th ACM Conference on Information-Centric Networking*, ICN '22, page 125–136, New York, NY, USA, 2022. Association for Computing Machinery.
14. Loren Kohnfelder. *Designing Secure Software*. No Starch Press, 2021.
15. Sara Montagna, Stefano Ferretti, Lorenz Cuno Klopfenstein, Antonio Florio, and Martino Francesco Pengo. Data decentralisation of llm-based chatbot systems in chronic disease self-management. In *ACM Conference on Information Technology for Social Good*, GoodIT, New York, NY, USA, 2023.
16. Georgios Mylonas, Athanasios Kalogeras, Sobah Abbas Petersen, Luis Muñoz, and Ioannis Chatzigiannakis. When circular economy meets the smart city ecosystem: Defining the smart and circular city, 2024.
17. Francesco Aurelio Pironti, Francesco Blefari, and Angelo Furfaro. Supporting C2C communications in a smart shire environment using DLT-based data mules. In *International Conference on Future Internet of Things and Cloud (FiCloud)*. IEEE, 2024.
18. Tina Ringenson, Elina Eriksson, Miriam Börjesson Rivera, and Josefin Wangel. The limits of the smart sustainable city. In *Proceedings of the 2017 Workshop on Computing Within Limits*, LIMITS '17, page 3–9, New York, NY, USA, 2017. Association for Computing Machinery.
19. Luca Serena, Moreno Marzolla, Gabriele D'Angelo, and Stefano Ferretti. Multilevel modeling as a methodology for the simulation of human mobility. In *IEEE/ACM International Symposium on Distributed Simulation and Real Time Applications (DS-RT)*, 2022.
20. Mirko Zichichi, Luca Serena, Stefano Ferretti, and Gabriele D'angelo. InDaMul: Incentivized data mules for opportunistic networking through smart contracts and decentralized systems. *ACM Distributed Ledger Technologies: Research and Practice*, 2(2), June 2023.

**Francesco Blefari** is a Ph.D. candidate in Cybersecurity at the University of Calabria and the IMT School for Advanced Studies Lucca. His research focuses on cyber ranges, binary analysis, web security and cybersecurity of LLM. Contact him at: francesco.blefari@unical.it.

**Gabriele D'Angelo** is an Assistant Professor (tenured) at the Department of Computer Science and Engineering of the University of Bologna. He has been a visiting researcher at the Université Paris Diderot, Laboratoire Preuves, Programmes et Systèmes (Paris, France) and at the School of Computing, National University of Singapore (NUS) (Singapore). His research interests include cybersecurity, simulation, blockchains, and cryptocurrencies. Contact him at: g.dangelo@unibo.it.

**Stefano Ferretti** is a Full Professor at the Department of Computer Science and Engineering of the University of Bologna. His current research interests

include distributed systems, complex networks, data science and blockchain technologies. Contact him at: s.ferretti@unibo.it.

**Angelo Furfaro** is an Associate Professor of Computer Engineering at the Department of Computer Engineering, Modeling, Electronics, and Systems (DIMES), University of Calabria, Rende (CS), Italy. He leads the CyberSec Lab at the University of Calabria and currently serves as Editor-in-Chief of Simulation Modelling Practice and Theory (Elsevier). His research interests include cybersecurity, simulation, and software engineering. He is a Senior Member of the IEEE. Contact him at: angelo.furfaro@unical.it.

**Paolo Giaccone** is Full Professor in the Department of Electronics, Politecnico di Torino. During 2000-2001 and in 2002 he was with the Information Systems Networking Lab, Electrical Engineering Dept., Stanford University, Stanford, CA. His main area of interest is the design of network algorithms, in particular for SDN networks and cloud computing systems. He is a Senior Member of IEEE. Contact him at: paolo.giaccone@polito.it.

**Moreno Marzolla** is Associate Professor at the Department of Computer Science and Engineering, University of Bologna, Italy. His research interests include systems performance modeling, parallel and distributed algorithms, and complex systems analysis. Contact him at: moreno.marzolla@unibo.it.

**Francesco Aurelio Pironti** is a Ph.D. student specializing in Industrial Control Systems (ICS) and Internet of Things (IoT) security. Contact him at: francesco.pironti@unical.it.

**Luca Serena** is a research fellow at the Department of Computer Science and Engineering, University of Bologna, Italy. His research interests include simulation, cybersecurity, complex networks, and distributed ledger technologies. Contact him at: luca.serena2@unibo.it.