

The SERS framework: a stakeholder-oriented approach to designing and evaluating distributed ledger systems

Fatemeh Esmaeilnezhadtanha, Aliakbar Hasani , Luca Spalazzi & Yves Wautelet

To cite this article: Fatemeh Esmaeilnezhadtanha, Aliakbar Hasani , Luca Spalazzi & Yves Wautelet (29 Jul 2026): The SERS framework: a stakeholder-oriented approach to designing and evaluating distributed ledger systems, Journal of Information and Telecommunication, DOI: [10.1080/24751839.2026.2707673](https://doi.org/10.1080/24751839.2026.2707673)

To link to this article: <https://doi.org/10.1080/24751839.2026.2707673>



© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 29 Jul 2026.



Submit your article to this journal [↗](#)



View related articles [↗](#)



View Crossmark data [↗](#)

The SERS framework: a stakeholder-oriented approach to designing and evaluating distributed ledger systems

Fatemeh Esmaeilnezhadtanha ^{a,b,c}, Aliakbar Hasani^d, Luca Spalazzi^b and Yves Wautelet ^c

^aSchool of Advanced Studies (SAS), University of Camerino, Camerino, Italy; ^bDipartimento di Ingegneria dell'Informazione (DII), Università Politecnica delle Marche, Ancona, Italy; ^cDepartment of Industrial Engineering and Management, KU Leuven, Leuven, Belgium; ^dFaculty of Economics and Business (FEB), Shahrood University of Technology, Shahrood, Iran

ABSTRACT

Distributed ledger technology (DLT) initiatives are frequently designed from a predominantly technical and functional perspective. Such a narrow focus often overlooks stakeholder-oriented non-functional requirements, thereby limiting adoption in complex socio-technical environments. To address this gap, this paper develops the SERS framework, a stakeholder-oriented framework that structures four key dimensions for the design and evaluation of decentralized systems: Security, Efficiency, Resiliency, and Sustainability. Following a Design Science Research approach, the framework is derived from a systematic literature review and refined through expert validation using the fuzzy Delphi technique. The resulting framework provides a domain-independent typology of stakeholder-oriented performance dimensions and associated assessment criteria. To demonstrate its applicability, the framework is used to guide the design of a multi-layer architecture integrating distributed ledger technologies, IoT, and Cloud/Edge/Fog computing within a healthcare context. The architecture is subsequently evaluated using the Fuzzy Analytic Network Process (Fuzzy-ANP) based on the SERS dimensions. The results indicate that the proposed architecture performs particularly strongly in terms of security and resiliency, while highlighting efficiency and sustainability as areas requiring further improvement. Beyond healthcare, the SERS framework provides a reusable mechanism for designing and evaluating decentralized socio-technical systems across a broad range of technology adoption contexts.

ARTICLE HISTORY

Received 14 January 2026
Accepted 17 July 2026

KEYWORDS

Design science research;
fuzzy delphi method;
assessment framework;
multi-layered system
architecture; blockchain;
non-functional requirements

1. Introduction

Over the last years, Distributed Ledger Technologies (DLTs) such as blockchain have been introduced across many domains, often with a strong emphasis on innovation in smart technology-driven systems (Alt & Gräser, 2025). While these innovations have brought significant benefits, they have also revealed persistent shortcomings: systems are too often

CONTACT Yves Wautelet  yves.wautelet@kuleuven.be  Warmoesberg 26, 1000 Brussel, Belgium

© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

engineered from a purely technical perspective, with limited consideration of stakeholder needs and non-functional requirements (Bauer et al., 2023). In addition, as highlighted in (Esmaeilnezhadtanha et al., 2025), DLT within the specific field of healthcare faces adoption challenges that extend well beyond technical scalability and consensus, encompassing efficiency, privacy protection, regulatory compliance, interoperability, and alignment with domain-specific practices such as patient- and physician-centred care. These findings underscore that effective integration requires frameworks that explicitly embed stakeholder needs and non-functional requirements into system design. Without such a stakeholder-driven approach, DLT initiatives risk remaining at the pilot stage, despite their promise of decentralization and trust.

More specifically, DLT systems, especially when they are combined with other technologies like IoT, are characterized by numerous data sources and complex data structures, which intensify long-standing concerns around encryption, digital signatures, immutable records, and low-latency pipelines (Abbasi et al., 2023). While these technical requirements are critical, they do not by themselves ensure solutions that are resilient, sustainable, or broadly adopted in stakeholder-intensive contexts (Hasani & Haseli, 2024). We thus suggest building a systematic approach that typologizes key non-functional requirements and designs the architecture of such systems in a way that sustains these. In response to this need, this study is guided by the following key research questions:

1. *How to design a comprehensive framework that structures security, efficiency, resiliency, and sustainability into typologies and clearly specifies their dimensions for assessment?*
2. *How can such a framework guide the systematic architectural development of technology-driven systems?*

These research questions are meant to lead to two distinct contributions. First, the need to develop an evaluation framework that can be used as a reference for building stakeholder-aware technical systems. Second, showing the relevance of that framework by using it as a guide for the design of an architecture integrating DLT, IoT, and Cloud/Edge/Fog computing. In order to demonstrate the relevance of the first contribution on the design of the second, we proceed to an ex-post re-evaluation of the performance of the architecture on the elements distinguished in the first one.

The remainder of this paper is organized as follows. Section 2 provides the theoretical background on distributed ledger technologies, IoT systems, and Edge/Fog/Cloud computing, which constitute the technological foundations of the study. Section 3 presents the research methodology and details the Design Science Research process used to develop and evaluate the proposed artefacts. Section 4 introduces the SERS framework and the multi-layer architecture designed to operationalize its dimensions. Section 5 presents the application and validation results obtained through the Fuzzy-ANP evaluation. Section 6 discusses the findings in relation to existing research and highlights the contributions of the study. Finally, Section 7 concludes the paper, outlines its limitations, and identifies directions for future research.

2. Theoretical background

This section introduces the technological foundations that underpin the proposed SERS framework and the multi-layer architecture developed in this study. Since the objective

is to design and evaluate stakeholder-oriented distributed systems, it is necessary to understand the architectural principles of distributed ledger technologies (DLTs), Internet of Things (IoT) ecosystems, and Edge/Fog/Cloud computing. These technologies are increasingly combined to support decentralized, data-intensive applications. The following subsections review their key architectural characteristics.

2.1. DLT Architecture

A DLT system is a decentralized and widely replicated database (i.e. the ledger) used to manage and store transactions. Each transaction is validated by a community of validators, and once consensus is reached, the transaction is broadcast via a peer-to-peer (P2P) protocol and stored immutably across all copies of the ledger. Typically, the DLT architecture is depicted as in Figure 1(a) (Acharya et al., 2019; Birje et al., 2022; Tabatabaei et al., 2023).

Briefly, the infrastructure layer contains for each validator all the infrastructures it needs to accomplish its tasks. The data layer deals with data structures that are used for implementing the ledger; usually, they are blockchains or hash graphs. The next layer deals with broadcasting transactions over the community of validators according to a P2P protocol. In other words, it assures that nodes can find and connect to each other, exchange data, and work together to maintain the precise and current state of the blockchain network.

The consensus layer oversees confirming the blocks, placing them in the proper sequence, and making sure that everyone agrees. On top of such layers, the smart contract layer deals with the decentralized execution of pieces of code (the smart contracts), namely, when a request of run a given method of a smart contract arrives, each validator runs the same piece of code. This is based on the underlying layers to ensure that a

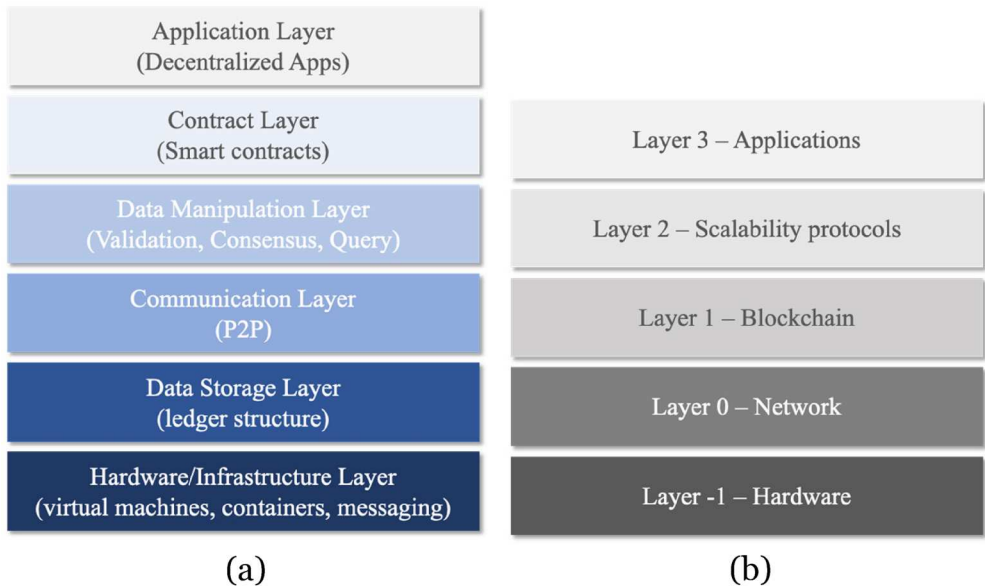


Figure 1. (a) DLT layered architecture. (b) Scalable blockchain layered architecture (authors' own contribution).

consensus is reached on the result. This part of a software application is called the on-chain component. Finally, the application layer is the part of a software application that interacts with smart contracts on one side and with users and the external world on the other side. It is usually referred to as the off-chain component of the application.

Given the absence of both a single point of authority (decisions are made only if consensus is reached) and a single point of failure (high redundancy) in this type of architecture, DLTs are well-suited to meet the *security* and *resilience* constraints. However, this very high level of redundancy leads to a ‘waste’ of resources, thus raising *sustainability* issues, and consensus lengthens decision times, reducing scalability. For this very reason, recent studies have focused on Layer-2 (L2) DLTs, designed specifically to solve these problems. L2 solutions are fundamentally based on the idea of distributing the workload among different (so-called) Layer-1 (L1) DLTs (i.e. the traditional DLTs). Therefore, these types of solutions are often represented by a layered architecture as in Figure 1 (b) (Antonio et al., 2024; Gangwal et al., 2023).

In parallel with L2 developments, DLT has emerged as a key enabler for enhancing trust, transparency, and data integrity in decentralized environments (Obaidat et al., 2024). For instance, a blockchain operates as a distributed ledger in which transactions are grouped into cryptographically linked blocks, ensuring immutability and verifiable provenance. Each transaction is digitally signed by its originator, providing accountability and non-repudiation. The replicated and decentralized nature of blockchain networks guarantees high availability and fault tolerance while removing the need for centralized intermediaries (Al-Matari et al., 2024).

2.2. IoT and edge/fog/cloud architectures

IoT refers to a network of physical objects equipped with sensors, software, and other technologies that allow them to connect and exchange data over the Internet. The IoT reference architecture is depicted in Figure 2 (a) (Burhan et al., 2018).

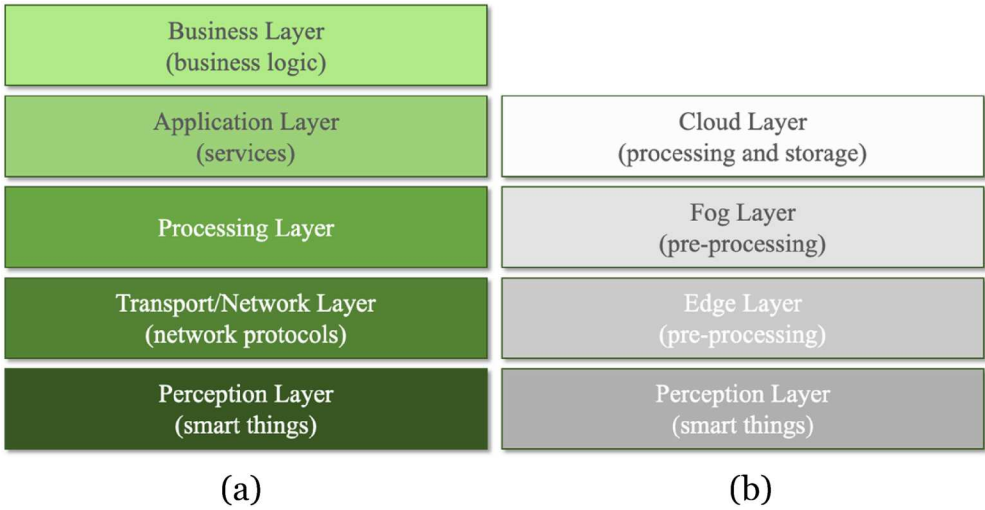


Figure 2. (a) IoT layered architecture. (b) Edge/fog/cloud layered architecture (authors’ own contribution).

The layered view of the IoT reference architecture, as outlined in the literature, traditionally places the perception layer at the lowest level, where the sensors and smart objects to be connected are located. The connection of these objects is managed in the transport layer. This raw data, once collected, is typically processed in the processing layer to feed applications. These applications are typically part of business processes in the business layer.

The exponential expansion of the IoT has resulted in vast volumes of heterogeneous data generated at the network periphery, creating new challenges in terms of sustainability, latency, bandwidth utilization, security, and trust management (Gu et al., 2023). Traditional cloud-centric architectures, while offering substantial storage and computational resources, often encounter performance bottlenecks due to the transmission of massive data streams to distant data centres (Shi et al., 2016).

Scalability issues have also emerged in the IoT area. It was quickly realized that processing the enormous amount of raw data arriving from sensors at once presents significant scalability challenges. For this reason, a multi-layer architecture for computing-intensive IoT applications was proposed (Firouzi et al., 2021; Muneeb et al., 2021; Oliveira et al., 2022) (see Figure 2 (b)), where initial processing occurs where the data is collected (edge layer), taking advantage of the existing intelligent objects; a second processing occurs close to the data collection point (fog layer), leveraging the gateways used to route the data across the Internet; this allows only a smaller set of (processed) data to reach the processing layer (cloud layer), reducing network traffic and cloud processing costs. This multi-tiered architecture ensures efficient, scalable, and context-responsive data management across distributed IoT systems (Oliveira et al., 2022).

Finally, IoT-DLTs are well-suited to meeting the *efficiency, resiliency, and sustainability* constraints. When DLT and edge/fog/cloud computing are integrated, a synergistic framework emerges: DLT provides the trust and traceability layer, while edge, fog, and cloud nodes manage the computational and storage demands of massive IoT data streams (Obaidat et al., 2024). This interaction typically follows an on-chain/off-chain paradigm, where the DLT (on-chain) is employed to record verifiable proofs of transactions, identities, and data integrity, while the bulk of data storage and processing occurs across the edge/fog/cloud continuum (off-chain) (Eren et al., 2025). This division of responsibilities enables scalable, secure, and efficient IoT ecosystems that can support autonomous operation, verifiable data exchange, and resilient decision-making in diverse application domains.

3. Research methodology

A Design Science Research (DSR) approach (Hevner et al., 2004) is followed for creating the main artefacts of this study, which are the contributions:

- The primary artefact (called the SERS framework in the rest of this paper) is a novel, domain-independent framework for designing and evaluating the stakeholder-based performance of technological systems;
- The secondary artefact is the multi-layer system architecture for integrating DLT, IoT, and edge/cloud/fog, demonstrating the applicability of the framework developed as the primary artefact. The architecture serves as a proof-of-concept.

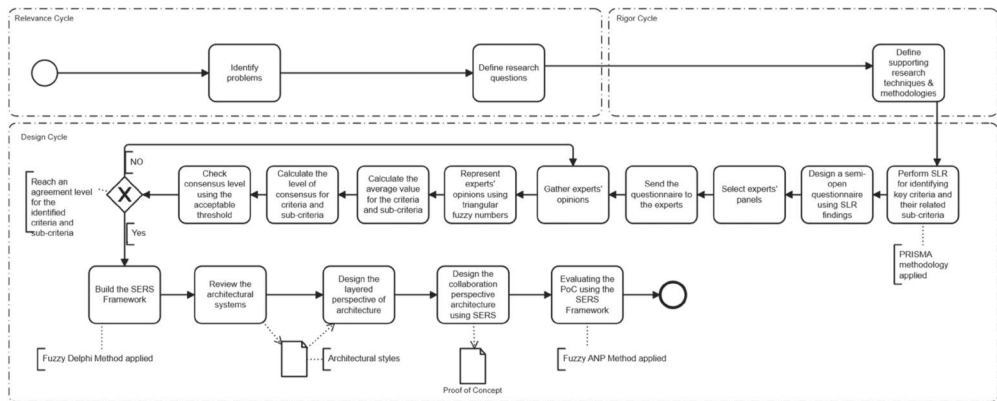


Figure 3. Research workflow.

Figure 3 depicts this research workflow: the relevance, rigour, and design cycles leading to the construction of these two artefacts are further depicted in this section.

3.1. Relevance cycle

The relevance cycle covers the identification of problems and opportunities in the application domain (Wautelet & Rouget, 2025). Recent studies (Al-Matari et al., 2024; Eren et al., 2025; Obaidat et al., 2024) have shown that the adoption of DLTs into real-world implementations remains limited because their development is guided primarily by technical and functional considerations. Esmailnezhadtanha et al. (Esmailnezhadtanha et al., 2025) have shown that the rapid diffusion of interconnected and decentralized technologies, such as the IoT and DLTs, has generated high expectations regarding their potential to enhance resiliency and efficiency, address security issues such as privacy, and improve sustainability across the studied domain. In domains such as healthcare, where adoption depends not only on technical performance but also on sustainability, security, and long-term resilience, this narrow focus undermines trust and limits efficiency. Without a comprehensive view that integrates these concerns, DLT projects risk remaining pilot exercises rather than achieving sustainable deployment.

This situation points to a clear research gap: *the lack of structured frameworks that bring together the different non-functional, i.e. stakeholder-oriented requirements in a systematic way, so that they can support both the design and evaluation of technical systems*. Existing research stresses the need to move beyond fragmented treatments of isolated issues towards integrative approaches that capture the full range of expectations stakeholders place on solutions like DLT. Addressing this gap is essential to improve adoption, particularly in stakeholder-intensive domains such as healthcare, where technical soundness alone is insufficient to ensure legitimacy, trust, and long-term impact.

Also, the rapid growth of interconnected ecosystems is reflected in recent estimates that nearly 18.8 billion IoT devices are connected (Gu et al., 2023). The enormous amount of data generated in these environments necessitates edge/fog/cloud solutions and raises new challenges regarding privacy, trust, traceability, and transparency.¹ While DLTs appear to offer an effective trust layer through immutable notarization and

decentralized execution, their adoption continues to grow. Furthermore, there has been an increase in work aimed at integrating DLT with IoT (Al-Matari et al., 2024; Eren et al., 2025; Obaidat et al., 2024). This integration is a domain in which we can witness the need for systems that better support stakeholder perspectives. To technically achieve this, we suggest developing a layered architecture that integrates these technologies as interdependent layers. This newly designed multi-layered architecture shows a concrete implementation possibility of the non-functional requirements identified in the first contribution.

3.2. Rigour cycle

The rigour cycle refers to the methods and theories used to ground the construction and assessment of the two artefacts (Hevner et al., 2004; Wautelet & Rouget, 2025). This section summarizes the techniques, methods, and frameworks used.

To come up with the building of the SERS framework, we conducted a hybrid research strategy. More precisely, the framework is developed by applying the systematic literature review method, through PRISMA guidelines (Page et al., 2021), to identify the dimensions relevant for stakeholders when adopting new technology. Then, we used a multi-stage expert-driven process to collect viewpoints regarding validating the dimensions, and the results were analysed using the Fuzzy Delphi method (Hasani et al., 2025; Ishikawa et al., 1993). A questionnaire is used to gather experts' views on the acceptability of the criteria and subcriteria and to assess whether their number is appropriate, comprehensive, and not excessive. At this step, the experts reviewed the definitions of each criterion and sub-criterion. They were asked to check whether the proposed set of sub-criteria for each criterion is acceptable. To gauge agreement among the experts, we used a formal metric to quantify the level of consensus.

Building of the second artefact (i.e. the reference architecture related to the integration of IoT, edge/fog/cloud computing, and DLT), to ensure methodological robustness, all architectural decisions were based exclusively on recognized and validated scientific knowledge. First, we adopted classical software engineering practices, systematic literature analysis, reference model extraction, and layer decomposition, anchored in the foundational theory of software architecture formalized by Kruchten (1995) and Perry & Wolf (1992). These works provide the scientific basis for using layered architecture, a style whose properties (modularity, separation of concerns, maintainability) are well established and widely accepted. Second, instead of proposing ad-hoc models, we grounded the artefact in canonical reference architectures from the literature: the standard DLT/L1/L2 stacks (Acharya et al., 2019; Birje et al., 2022; Gangwal et al., 2023; Tabatabaei et al., 2023), the traditional IoT layered architecture (Burhan et al., 2018), and the consolidated edge–fog–cloud model (Muneeb et al., 2021).

Third, the integration was executed using established architectural synthesis techniques, particularly layer correspondence mapping and functional alignment, consistent with IEEE 42010 guidelines. Finally, the architecture was validated through a healthcare scenario, providing a domain-specific viewpoint to assess its alignment with the SERS requirements. Overall, methodological rigour was achieved by basing the artefact exclusively on authoritative architectural theory, widely recognized reference models, and systematic, reproducible integration procedures. This means that we started from

requirements engineering, then we designed the architecture. Finally, the second artefact is evaluated by applying the Analytic Network Process (ANP) technique (Hasani & Haseli, 2024) to determine the relative importance of the considered framework criteria and sub-criteria.

3.3. Design cycle

In the design cycle, two artefacts were systematically constructed and evaluated to address the research questions.

3.3.1. Development of the SERS framework (Artefact 1)

The first artefact centred on developing the SERS performance assessment framework. This began with an SLR (Esmailnezhadtnha et al., 2025). The literature review was conducted on two of the most important scientific databases (Scopus® and PubMed®), looking for publications on DLTs and healthcare. The following query was used: (block-chain OR dlt OR «distributed ledger» OR «smart contract») AND (health OR healthcare).

At this point, the gathered papers were screened according to the following inclusion criteria:

- the works aim at using DLT in a healthcare scenario,
- the works contain enough information to answer our Research Questions,
- the works describe a specific use case,

and the following exclusion criteria:

- the works are reviews or surveys,
- the proposed systems were not experimented.

The SLR was used to establish a comprehensive set of criteria and sub-criteria relevant to evaluating smart, technology-driven systems. These initial findings were iteratively refined through expert validation using the fuzzy Delphi method (Hasani & Haseli, 2024; Ishikawa et al., 1993), enabling the consolidation, clarification, and prioritization of the measures. The result of this cycle was a validated and rigorously structured framework that reflected expert consensus on the essential dimensions of security, efficiency, resiliency, and sustainability.

The fuzzy Delphi technique was employed as a structured, group-based communication process, enabling experts to assess and refine complex problems through iterative consensus-building independently. The expert panel consisted of 17 experts from academia and healthcare-related disciplines across six countries. The panel combined expertise in distributed ledger technologies, information systems, digital health, healthcare informatics, cybersecurity, artificial intelligence, and technology adoption. Participants occupied positions ranging from Associate Professor to Full Professor and collectively represented substantial experience in both information technology and distributed ledger technologies. Table 1 summarizes the profile of the participating experts.

This validation occurred in two consecutive stages. In the first stage, a semi-open questionnaire derived from the SLR results was distributed to domain experts. The experts

Table 1. Profile of experts participating in the fuzzy Delphi validation process.

Education	Affiliation	Country	Current Position	Fields of Expertise	Years in Academic Position	Years of IT Expertise	Years of DLT Expertise
Ph.D. in Information Technology Management	Florida International University	U.S.A.	Associate Professor	Blockchain and cryptocurrency adoption, IoT in healthcare	9	21	7
Ph.D. Computer Science	Vanderbilt University	U.S.A.	Full Professor and Chief Technology Officer	Adaptive distributed computing middleware for high-performance and real-time applications	30	30	7
Ph.D. in Civil Engineering	The University of Texas at Austin	U.S.A.	Professor	Information systems, data mining, project management, engineering economic analysis, and building construction	21	16	2
Ph.D. Computer Science and Information Systems	University of California San Diego	U.S.A.	Associate Professor of Biomedical Informatics and Data Science	Medical Informatics	10	21	8
Ph.D. Neurobiology and Neurosciences	Icahn School of Medicine at Mount Sinai	U.S.A.	Associate Professor	Health data science and machine learning, EHR, Digital Health	5	14	4
Ph.D. in modelling and simulation of human ventricular electrophysiology	Keble College, Oxford	England	Professor	Modelling and Simulation, Computational Cardiology	14	14	4
Ph.D. Computer Science	University of Southampton	England	Professor	Cyber Security	26	26	7
Ph.D. in Business and Economics	University of Iowa	U.S.A.	Professor	AI, business intelligence and analytics, data mining, text mining, social media analytics	22	26	4
Ph.D. in Business Administration and Management	University of North Carolina at Greensboro	U.S.A.	Professor	AI, generative AI, Blockchain, Metaverse, Web3	21	11	7
Hospital physician, postdoc in medical informatics and health technology assessment	University of Southampton	England	Professor	Digital Healthcare, effective clinical AI and decision support	19	14	N/A
Ph.D. in Information Technology	HEC Montréal	Canada	Professor	Digital Health, information systems	20	29	N/A
Ph.D. Public Health / Digital Health / Mental Health	University of Oxford / Jesus College	England	Professor	Digital health and AI	14	21	N/A
Postdoctoral Researcher in Digital Health	University of Potsdam	Germany	Professor	Digital Health – Connected Healthcare	11	11	N/A

(Continued)

Table 1. Continued.

Education	Affiliation	Country	Current Position	Fields of Expertise	Years in Academic Position	Years of IT Expertise	Years of DLT Expertise
Ph.D. in Healthcare Administration and Business Administration	Franklin University	U.S.A.	Adjunct Professor	Health Administration, Business Administration	2	4	N/A
Ph.D. Management Information Systems	University of Jordan	Jordan	Professor	Technology Adoption, Management Information Systems	13	14	1
Doctorate and Habilitation in Business Administration and Information Systems	University of Mannheim	Germany	Professor	IT Management, Healthcare IT, Digital Innovation, IT Outsourcing	25	25	N/A
Ph.D. Management of Technology	University of Audencia	France	Professor	Information Systems, Cloud Computing, Health IT, Policy and Technology	25	25	N/A

evaluated the identified criteria and sub-criteria in terms of their relevance, clarity, and importance, while also being encouraged to propose additional performance measures. Owing to the qualitative nature of these assessments, a fuzzy approach was adopted, where linguistic evaluations were represented using fuzzy triangular numbers.

The second-stage questionnaire was prepared based on the first-stage outcomes. Experts were asked to re-evaluate the refined set of criteria and sub-criteria to determine their relative importance. Consensus was achieved when the difference between the defuzzified averages of two consecutive Delphi rounds was less than 0.1, indicating convergence of expert opinions. The final output of this process was a validated framework comprising key performance assessment criteria and their associated sub-criteria. [Figure 1](#) illustrates the overall process of the applied fuzzy Delphi method.

The construction of the SERS framework involved several activities. Two complementary stages are particularly relevant for understanding the development and validation of the framework:

- The SLR described in (Esmailnezhadtanha et al., [2025](#)): Identification of holistic performance assessment criteria and sub-criteria.

Refinements were made to improve the clarity, definition, and relationships among measures. The SLR results indicated that information systems across various domains commonly face challenges related to:

- Security focuses on protecting data integrity and confidentiality through proactive defences and compliance.
 - Performance efficiency emphasizes reducing costs and maximizing resource use while ensuring service accessibility.
 - Resiliency capability ensures system continuity and rapid recovery during disruptions, with metrics like recovery time and redundancy effectiveness.
 - Sustainability concerns aim at minimizing waste and reducing environmental impact while optimizing resource use, ensuring operations are both ecologically and economically conscious.
- The Expert Validation via Fuzzy Delphi: Domain experts assessed the validity, completeness, and applicability of the framework.

The final version of the SERS framework was validated through this two-phase expert-driven process. All measures that met the acceptance threshold of 0.4 (Hasani & Haseli, [2024](#)) were verified and incorporated into the final framework. [Table 2](#) presents the resulting criteria and sub-criteria established through the fuzzy Delphi method.

3.3.2 Development of the multi-layer architecture (Artefact 2)

The activities described above contributed to the construction and validation of the SERS framework (first artefact). The SLR enabled the identification of stakeholder-oriented performance dimensions and associated criteria, while the fuzzy Delphi process provided expert validation of their relevance, completeness, and structure. The resulting validated

Table 2. Final results of fuzzy Delphi method for designing the SERS framework.

Criteria	Aggregated fuzzy evaluation	De-fuzzy evaluation
Accessible and affordable	(0.567,0.767,0.967)	0.767
Cost-effective	(0.400,0.600,0.800)	0.600
Optimized	(0.400,0.600,0.800)	0.600
Reliable	(0.533,0.733,0.933)	0.733
Recovery	(0.533,0.733,0.933)	0.733
Redundancy	(0.500,0.700,0.900)	0.700
Resourcefulness	(0.467,0.667,0.867)	0.667
Robustness	(0.500,0.700,0.900)	0.700
Defended	(0.367,0.567,0.767)	0.567
Protected	(0.600,0.800,1.000)	0.800
Strengthened	(0.500,0.700,0.900)	0.700
Tested	(0.433,0.633,0.833)	0.633
Focus on value-added core competencies	(0.567,0.767,0.967)	0.767
Reduce resource usage	(0.467,0.667,0.867)	0.667
Reduce the total operation cost	(0.433,0.633,0.833)	0.633
Reduce wastes	(0.433,0.633,0.833)	0.633
Accessible and affordable	(0.100,0.200,0.400)	0.267

framework subsequently served as the foundation for the design and evaluation of the second artefact, a multi-layer architecture integrating blockchain, IoT, and edge/fog/cloud computing.

Following validation, the identified performance assessment measures were consolidated into the SERS framework (Artefact 1). This validated framework served as the foundation for designing a second artefact: a comprehensive multi-layer architecture integrating blockchain with IoT-based edge, fog, and cloud systems. The framework was used both to guide architectural design and to define its subsequent evaluation. A second-stage questionnaire, derived from the validated SERS framework, was employed during this phase (it is presented in Appendix 1 after this paper; also the data collected during the interviews is available in an online appendix²).

To translate the SERS requirements into an architectural solution, the literature was systematically analysed to identify architectural styles capable of meeting the framework's performance criteria. This analysis revealed that layered architecture is one of the most widely adopted and well-established styles, owing to its clarity, modularity, and ease of design, maintenance, and scalability. Layered architectures have been applied successfully for decades, notably in network protocols, and were formalized in seminal reference works in the 1990s (Ambriola & Tortora, 1993; Kruchten, 1995; Perry & Wolf, 1992). As discussed in Section 2, layered architectures have also been adopted as reference models in distributed ledger technologies (DLT), IoT systems, and edge/fog/cloud computing.

Guided by the validated SERS framework and informed by existing reference architectures in DLT, IoT, and distributed computing, a unified multi-layer architecture was synthesized. The design aligns L1–L2 blockchain structures with the IoT and edge/fog/cloud stack by leveraging their shared layered principles. The architecture was tailored to the healthcare domain and instantiated as a proof-of-concept (PoC), ensuring that data acquisition, processing, and certified decision-making are consistently supported across layers. In this way, the second artefact operationalizes the SERS criteria by embedding their performance concerns directly into the architectural design.

3.3.3 Evaluation of the two artefacts

The final stage of the design cycle involved evaluating the instantiated multi-layer architecture using the SERS framework. This assessment, supported by fuzzy Analytic Network Process (ANP)³ techniques, systematically identified the strengths and limitations of the proposed architectural solution. The evaluation confirmed the practical utility of the SERS framework and provided deeper insights into how effectively the architecture satisfies the performance requirements derived from the SERS criteria. Collectively, the two artefacts were constructed, validated, and assessed in alignment with the overarching research objectives.

4. Results

In this section, the study's results are presented in response to the key research questions.

4.1. Developed SERS framework

As shown in [Figure 4](#), the final selected criteria of the SERS framework and their definitions, verified by experts, are as follows:

- **Security:** The security criteria could be assessed via the following sub-criteria:
 - Defended: The ability to respond to various cyber-physical attacks.
 - Protected: Ensuring an adequate level of protection, maintaining an effective proactive response to threats, and safeguarding against danger and harm.
 - Strengthened: The system ought to enhance security, particularly in relation to organizational processes.
 - Tested: The system should be evaluated in real-life conditions
- **Efficiency:** The efficiency criteria could be assessed via the following sub-criteria:
 - Accessible and Affordable: The ability to facilitate and make convenient access to services for everyone

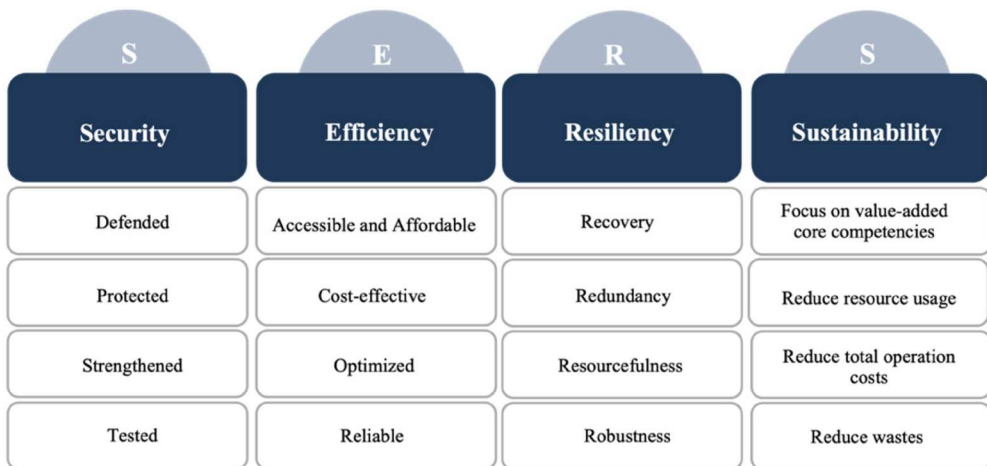


Figure 4. SERS Framework criteria and sub-criteria.

- Cost-effective: The ability to deliver optimal performance and benefits relative to its expenses.
- Optimized: The ability to improve the performance of services
- Reliable: Considered as reliability under various operational conditions.
- **Resiliency:** The resiliency criteria could be assessed via the following sub-criteria:
 - Recovery: The capability to quickly as well as efficiently return to normal status after a disruption occurs.
 - Redundancy: Considered as incorporating backup resources to support primary systems under failure.
 - Resourcefulness: The ability to find quick and clever ways to manage a disruption.
 - Robustness: The ability to preserve key operations under disruption.
- **Sustainability:** The sustainability criteria could be assessed via the following sub-criteria:
 - Focus on value-added core competencies: The capability that provides value within the service-providing system, enhances its competitive advantage, and delivers superior services to its stakeholders.
 - Reduce resource usage: The optimization of the utilization of resources such as energy, water, materials, and other inputs in the operations of the system.
 - Reduce total operation costs: The strategic effort of minimizing the overall expenses associated with the functioning of the healthcare system.
 - Reduce wastes: The focus is on implementing measures to minimize the generation of unnecessary waste materials within the system.

To facilitate interpretation of the framework and provide a concise overview of its dimensions, [Table 3](#) summarizes the definitions, associated sub-criteria, and representative architectural implications of the SERS framework.

Table 3. Overview of the SERS framework dimensions, associated sub-criteria, and representative architectural implications.

Dimension	Definition	Sub-Criteria	Illustrative Architectural Implications
Security	Protection of data, processes, and system assets against threats and unauthorized access.	Defended, Protected, Strengthened, Tested	Encryption, digital signatures, smart contracts, access control mechanisms, immutable records
Efficiency	Optimization of resources and service delivery while maintaining accessibility and reliability.	Accessible and Affordable, Cost-effective, Optimized, Reliable	Edge processing, workload distribution, reduced network traffic, optimized resource allocation
Resiliency	Ability to withstand disruptions and recover while maintaining essential operations.	Recovery, Redundancy, Resourcefulness, Robustness	Distributed ledger replication, fault tolerance, backup nodes, decentralized decision-making
Sustainability	Long-term economic and environmental viability through responsible resource management.	Focus on Value-Added Core Competencies, Reduce Resource Usage, Reduce Total Operation Cost, Reduce Wastes	Layer-2 blockchain solutions, optimized computing resources, waste reduction, energy-conscious design

4.2. The multi-layered architecture

After reviewing the reference architectures for DLT (L1 and L2), IoT, and edge/fog/cloud computing, the next task involves defining a reference architecture for an application that integrates DLT on the one hand and IoT-based edge/fog/cloud computing on the other. The process unfolds in three stages.

The first step involves defining an architecture that integrates Layers 1 and 2 of a DLT. Considering that an L2 DLT includes multiple L1 DLTs, it can be noticed that Layers –1, 0, and 1 in [Figure 2](#) (b) synthetically represent the layers in [Figure 2](#) (a). From this mapping, we obtain the layer stack shown on the left in [Figure 6](#) (the blue side).

The construction of the proposed architecture followed a three-step synthesis process. First, the reference architectures of Layer-1 and Layer-2 DLT systems were analysed to identify their core functional layers. Second, the reference architectures of IoT and edge/fog/cloud computing were examined to determine their respective data acquisition, communication, processing, and service responsibilities. Third, functional correspondences and integration points between these architectural layers were identified, resulting in a unified architecture capable of operationalizing the SERS dimensions.

The second step involves defining an architecture that integrates IoT with edge/fog/cloud computing. This integration naturally follows from the fact that the edge/fog/cloud architecture was originally conceived as a decomposition of the IoT processing layer into three distinct layers located at different points of the network. This leads to the layered architecture on the right in [Figure 5](#) (the green side).

The third step concerns the final integration, or how the two families of technologies interact with each other. [Figure 5](#) provides an abstract representation of this integration, simply by placing the two stacks of layers side by side.

A more detailed description of the interaction is provided in [Figure 6](#). This diagram captures the collaboration perspective and was obtained by considering the application domain: the healthcare scenario.

In the healthcare landscape, as previously mentioned, it is vitally important to collect patient data using appropriate sensors and process this information to keep doctors updated on patient status, prescribe new therapies, or modify existing ones. An IoT-based edge/fog/cloud architecture is well-suited to these tasks because the appropriately processed data reaches the cloud layer and is accessed from there by the application layer. From there, by traversing the architecture layers backwards, therapies can be adjusted as needed, reaching the devices (actuators) that implement them. However, in some cases, for example, an insulin pump whose infusion dosage depends on blood glucose levels measured by a glucometer, the process can be managed locally, directly at the edge and fog computing level.

These system features meet the efficiency, effectiveness, and sustainability requirements outlined in the SERS framework. Furthermore, any activity is notarized and certified by means of appropriate smart contracts that can operate at L1 of the DLT or L2 of the DLT. The use of DLTs meets the security and resiliency requirements in the SERS framework. The introduction of L2 in the architecture aims at meeting sustainability. Indeed, the workload is distributed among different L1 DLT systems whereas the L2 collects transaction summaries (the so-called rollups) to assure traceability and security saving space and time.

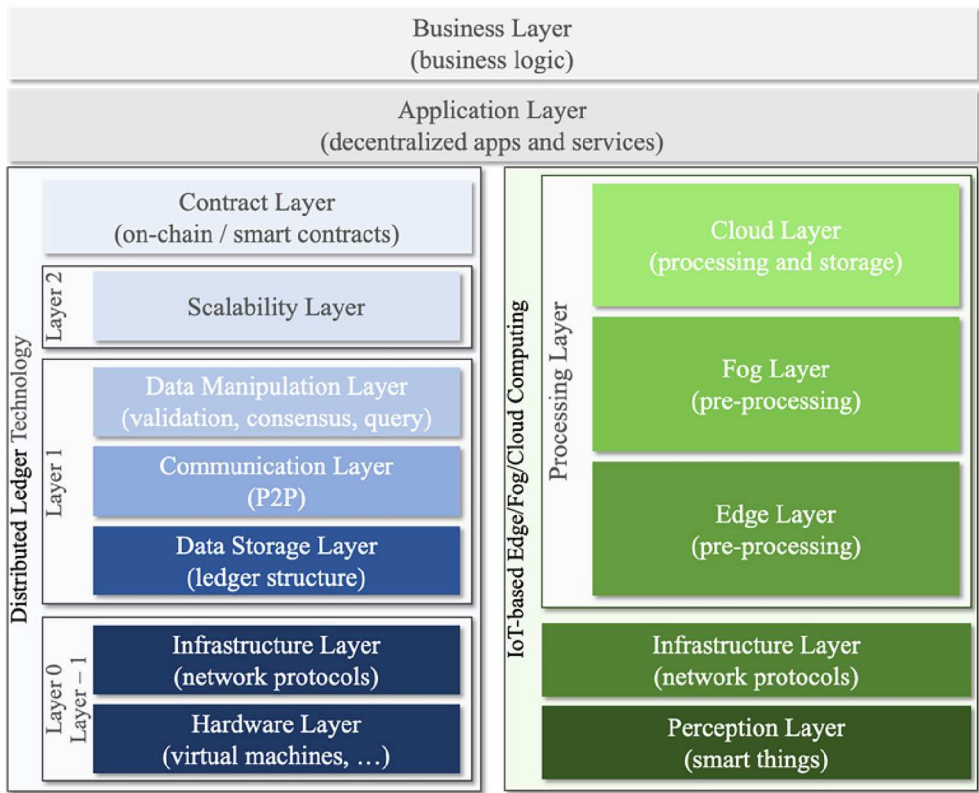


Figure 5. Blockchain Integration with IoT-based Edge/Fog/Cloud System. A layered perspective.

5. Application and validation of the proposed artefacts in a healthcare context

The developed SERS framework (artefact 1) is applied to evaluate the decentralized system, specifically the proposed multi-layer architecture (artefact 2). An essential element of discussion is the alignment procedure between the architecture and the SERS framework, ensuring that the system design and performance dimensions are coherently integrated. To achieve this, the ANP method is employed to establish the network structure based on the inner dependence relationships among sub-criteria and criteria, as well as the outer dependence relationships among the criteria and sub-criteria. Through this iterative process, the SERS framework has been refined to ensure its reliability and generalizability for evaluating decentralized systems.

The evaluation results of the network SERS index using the fuzzy network process analysis method are presented in Figure 7. These results are structured into two main parts: (1) the total importance of each criterion and sub-criterion, and (2) the overall performance of the proposed smart healthcare network. The evaluation outcomes for sustainability, efficiency, resiliency, and security, the four primary SERS criteria, are shown in Figure 8.

In terms of efficiency, the findings highlight the high priority of availability compared to other efficiency sub-criteria. This reflects the key function of a healthcare network –

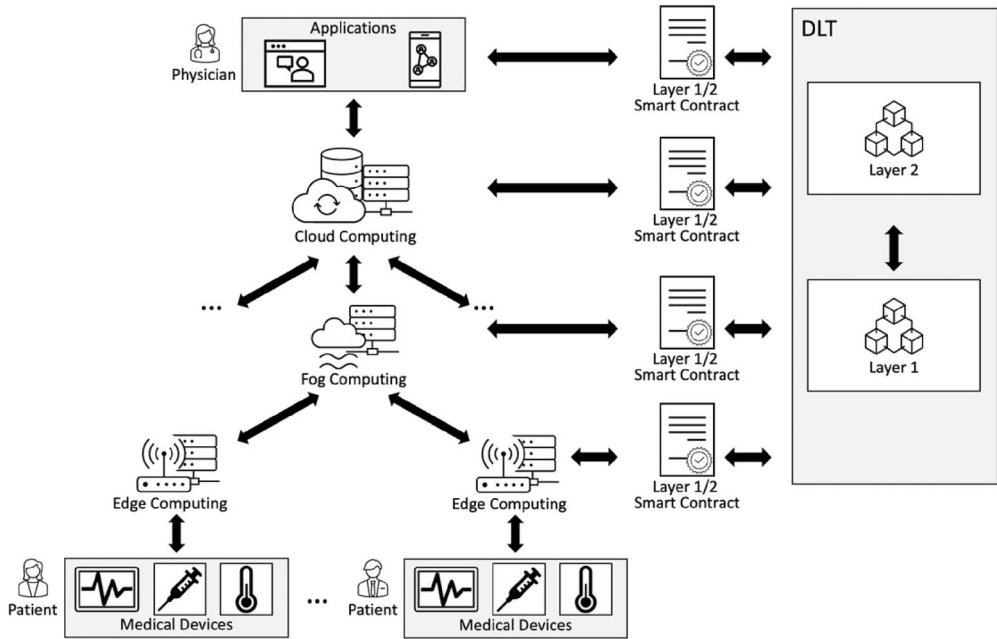


Figure 6. Blockchain Integration with IoT-based Edge/Fog/Cloud System. A collaboration perspective.

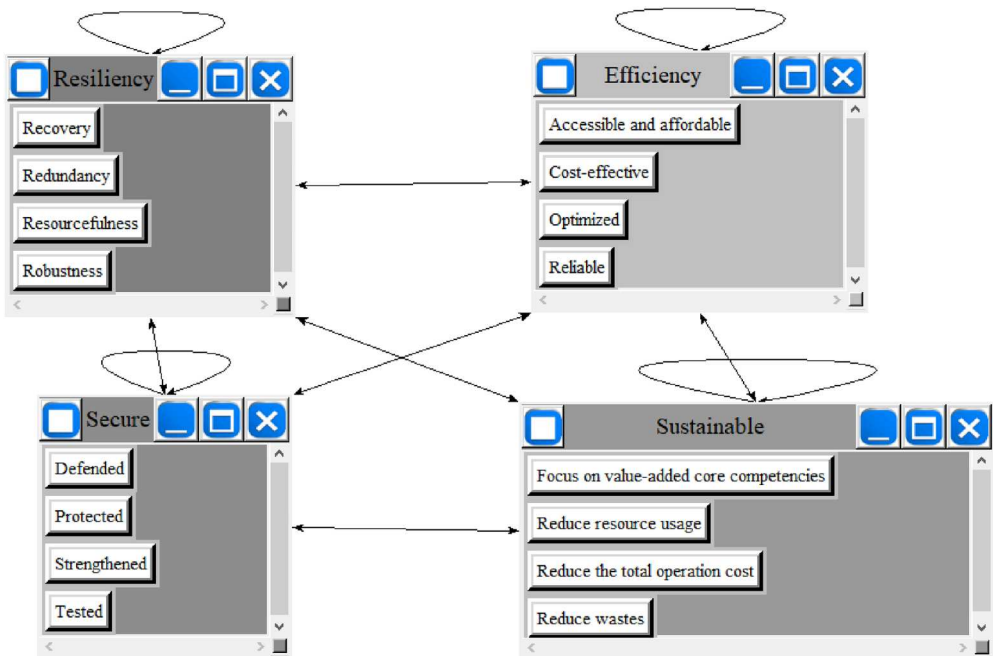


Figure 7. The network model structure of the proposed SERS assessment model.

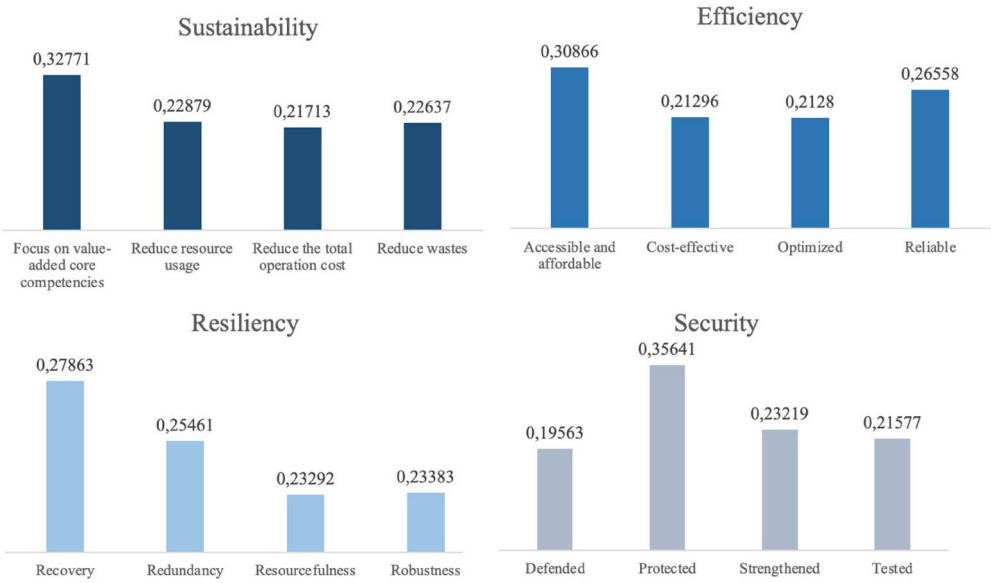


Figure 8. Results of healthcare network performance in terms of considered sub-criteria of the SERS model.

ensuring broad accessibility and continuous service provision. The second most important factor is reliable service delivery, which is closely tied to efficiency through uninterrupted and accurate healthcare operations. Integrating IoT and blockchain technologies within a unified system allows complementary functionalities that significantly enhance security, a major challenge in IoT-based environments. The design of a cost-effective and optimized healthcare network ranks third in efficiency assessment.

From a sustainability perspective, the most critical factor is the focus on core competencies to maximize value creation throughout the healthcare value chain. By integrating blockchain with IoT technologies, resource utilization can align with healthcare’s primary objectives, enabling waste reduction through disintermediation and digital transformation. This leads to improved resource efficiency, lower operational costs, and minimized waste generation, representing a sustainable model for digital healthcare transformation. Consequently, the measures related to reduced resource use, lower operational costs, and waste reduction are considered equally important.

For resiliency, smart healthcare systems must operate effectively under changing and unpredictable conditions without relying on a centralized control point. The integration of blockchain with IoT introduces decentralized data management through a peer-to-peer network and consensus mechanisms, enhancing recovery performance, which emerged as the most important resiliency criterion. The redundancy measure follows, reflecting the distributed nature of blockchain, which records transactions across multiple nodes. Together, these features ensure system robustness and the ability to maintain continuous functionality and service availability, even under adverse conditions.

Regarding security, smart healthcare networks must demonstrate active and adaptive responses to potential threats. Cybersecurity is a critical concern, and the use of smart contracts within blockchain implementations enhances the protection of healthcare

systems. Smart contracts facilitate secure and efficient processes for patient data management, healthcare transactions, drug supply chains, and integration with wearable IoT devices. The high importance of privacy and data protection underscores the need to safeguard the network from cyber-attacks and disruptions while maintaining cost-effective system protection aligned with other SERS dimensions, efficiency, resiliency, and sustainability. Other sub-criteria within security are also considered of equal importance and should be addressed comprehensively in smart healthcare system design.

The architecture was validated through expert review, where blockchain and IoT specialists assessed its alignment with the SERS performance dimensions. The experts confirmed that the designed system effectively integrates the SERS framework within the decentralized architectural model. The final evaluation results of the network SERS index using the fuzzy network process analysis are illustrated in [Figure 9](#), representing the overall criteria synthesis.

The results indicate that resiliency and security hold the highest importance in the proposed smart healthcare network. Blockchain, as a disruptive digital technology, introduces unparalleled levels of trust, transparency, and resilience. However, there remain significant opportunities for improvement in sustainability and efficiency. Technical challenges, such as the high cost of blockchain infrastructure, energy consumption, and hardware/software demands, can limit efficiency and scalability. Moreover, organizational and legal challenges, including the need for skilled personnel and adequate regulatory frameworks, affect the accessibility and optimization of blockchain implementation in healthcare systems.

In conclusion, while the integration of blockchain and IoT technologies significantly strengthens the resiliency and security aspects of decentralized healthcare systems, further improvements in sustainability are essential. This is particularly linked to the need for clean and affordable energy sources, as the increasing number of blockchain nodes amplifies energy consumption and environmental impact. Addressing these challenges will be crucial to ensure the holistic alignment of the architecture with the SERS framework, ultimately advancing the development of sustainable, efficient, resilient, and secure smart healthcare networks.

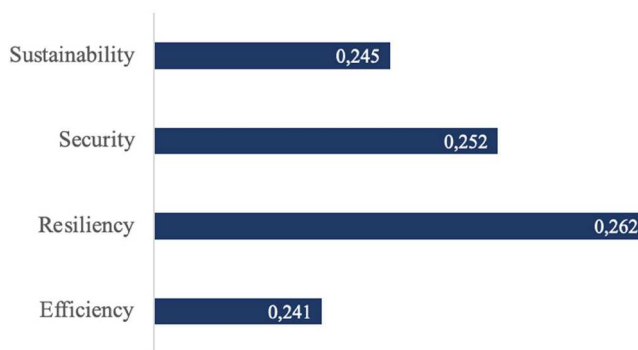


Figure 9. Final assessment of the proposed smart healthcare network based on the SERS criteria.

6. Related work

In this section, we compare our study with other related works to highlight the distinct contributions and improvements achieved through the SERS framework. While previous studies (Adere, 2022; Ahmad et al., 2022; Andrew et al., 2023; Gardas et al., 2022; Maden, 2019; Ramachandran, 2023) have primarily focused on isolated aspects such as data security, interoperability, or computational efficiency, our approach integrates these dimensions into a unified and comprehensive assessment model. Unlike traditional evaluations that emphasize either performance or reliability, our framework systematically combines technical, operational, and organizational criteria to ensure a balanced assessment of healthcare IT systems. This holistic approach enables a more accurate evaluation of technology adoption and long-term sustainability, addressing the gaps identified in prior research.

Broad surveys and architecture reviews have documented the promise and the recurring limitations of applying blockchain and IoT to healthcare, especially trade-offs among security, privacy, scalability, and operability, but most stop short of prescribing a domain-independent, multi-criteria evaluation embedded into system design (Ramachandran, 2023). Andrew et al. (2023) provided a thorough review of blockchain architectures and security challenges for healthcare summarizes technical gaps and open directions, but does not provide a unified non-functional assessment framework tied to a concrete multi-layer architecture.

Several prior studies tackle important pieces of the overall problem but in isolation. Adere (2022) provides a systematic literature analysis of blockchain and IoT for healthcare, emphasizing the benefits (privacy, tamper-resistance) and ongoing issues (interoperability, scalability), which aligns with our motivation but lacks a structured, stakeholder-driven non-functional criteria set and weighting process for system design.

Ahmad et al. (2022) present a fog-enabled IoT–blockchain healthcare architecture addressing latency and local responsiveness (critical engineering concerns), but their evaluation neglects requirements like security, resiliency, and sustainability.

Likewise, node-selection and trust mechanisms using fuzzy methods (e.g. Gardas et al., 2022, fuzzy node selection for blockchain-edge IoT) contribute useful technical mechanisms for efficiency and trustworthiness, yet they do not place those mechanisms within a comprehensive multi-criteria decision model that also captures organizational and sustainability concerns.

Other studies explore multi-criteria decision tools or sustainability/security engineering specifically for blockchain applications. Prior applications of fuzzy-ANP / ANP for suitability evaluation demonstrate how networked criteria and expert judgment can guide adoption decisions; however, these studies are typically applied to logistics or single-domain case studies rather than producing a reusable, domain-independent evaluation framework aligned with a concrete multi-layer blockchain–IoT–Cloud/Fog/Edge reference architecture. Similarly, proposals for secure as well as sustainable software engineering practices for healthcare blockchain begin to fold sustainability into engineering guidance but stop short of providing an integrated design and evaluation artefact validated via fuzzy-Delphi and fuzzy-ANP on a deployed multi-layer system (Maden, 2019).

Our work advances the state of the art by combining (1) an explicitly stakeholder-oriented, domain-independent SERS taxonomy (security, efficiency, resiliency,

sustainability) derived from a systematic literature review and validated via fuzzy-Delphi, (2) a dual artefact from design-science research, a reusable assessment framework plus a concrete multi-layer blockchain–IoT–Cloud/Fog/Edge architecture, and (3) a rigorous, network-aware evaluation using fuzzy-ANP that both weights interdependent sub-criteria and scores the implemented architecture. In short, whereas existing studies contribute valuable technical architectures, focused mechanisms (e.g. node selection or fog partitioning), or methodological approaches (e.g. fuzzy ANP applied in other domains) (Andrew et al., 2023), our contribution distinguishes itself by embedding stakeholder-oriented non-functional requirements into the system design lifecycle and demonstrating how these requirements influence architectural decisions and the evaluation of distributed ledger systems across the four SERS dimensions.

Beyond technical architectures, some studies have investigated blockchain adoption from an organizational and software engineering perspective. Conceptual modelling approaches have been proposed to capture stakeholder dependencies, privacy concerns, regulatory constraints, and organizational implications associated with blockchain-based ecosystems (Vingerhoets et al., 2021). While these approaches support the understanding and specification of blockchain-enabled systems, they do not provide a structured mechanism for evaluating stakeholder-oriented performance dimensions. This limitation motivates the development of the SERS framework.

As shown, several studies address some of these criteria in depth; however, to our knowledge, very few works address all of them together in the technology-driven setting.

7. Discussion

7.1. Applicability and Flexibility of the SERS Framework

An important element that deserves explicit discussion is the applicability of the SERS framework as a general structuring mechanism for technology adoption in stakeholder-intensive environments. While the framework is instantiated and validated through a distributed ledger-based use case, SERS is deliberately designed to be independent of any specific technological paradigm. The four core dimensions of security, efficiency, resiliency, and sustainability capture non-functional concerns that consistently shape adoption outcomes in complex socio-technical systems (so intensively executing technology to serve human stakeholders' needs). Consequently, SERS should not be understood as a blockchain-oriented evaluation model, but as a reusable analytical framework that supports any technology adoption customization across a broad range of digital transformation contexts.

From this perspective, SERS can for example be mobilized as a structuring approach for the adoption and integration of Artificial Intelligence (AI) with stakeholder-intensive environments. In AI-based applications, such as automated customer support or predictive analytics, the framework helps surface trade-offs between pure algorithmic gains in efficiency and core stakeholder needs as well as emerging risks related to security, system fragility, and long-term sustainability. More broadly, when AI is introduced as part of a larger digital transformation, the SERS dimensions can be reinterpreted to address concerns such as the robustness and security of data pipelines and models,

the system's ability to withstand and recover from operational disruptions, the efficiency and reliability of AI-enabled services under real-world conditions, and the long-term sustainability of AI capabilities in terms of resource usage, cost, and organizational value creation.

7.2. Use of the architecture and the gap towards implementation

The proposed multi-layer architecture serves as a reference architecture that illustrates how the SERS framework can be operationalized at a conceptual design level. Its purpose is not to function as a deployment-ready blueprint, but rather to demonstrate how non-functional requirements can be explicitly mapped onto architectural layers when integrating IoT, edge/fog/cloud computing, and DLT technologies.

A substantial gap remains between the reference architecture and an operational system. This gap manifests at multiple levels. First, there is an **engineering gap**, related to concrete implementation choices that are intentionally abstracted away in this study. These include the selection of specific blockchain platforms, consensus mechanisms, interoperability protocols, and performance optimization strategies. Second, there is a **governance gap**, concerning node ownership, operational responsibility, upgrade mechanisms, and accountability, issues that are central to the legitimacy of decentralized systems but lie beyond the scope of architectural abstraction. Third, a **regulatory gap** persists, particularly in domains such as healthcare, where data protection, liability, and compliance requirements directly constrain architectural choices. Finally, an **organizational gap** exists, involving cost structures, skill availability, and change management, all of which significantly influence technology adoption but cannot be resolved at the architectural level alone.

These gaps clarify the intended contribution of the architecture: its value lies in enabling stakeholders and designers to reason explicitly about *where* non-functional requirements are addressed, *why* certain technologies are introduced, and *which* concerns remain unresolved. In practical terms, the architecture can be used as a design aid to compare alternative solutions, identify unnecessary technological complexity, and justify architectural trade-offs.

8. Conclusion

The successful adoption of DLT and other emerging digital infrastructures does not only depend on technical performance but also on their ability to satisfy stakeholder-oriented values. Security, efficiency, resiliency, and sustainability play a critical role in determining whether technology-driven systems can be effectively embedded within complex socio-technical environments. Consequently, the design and evaluation of such systems require structured approaches capable of balancing technological capabilities with organizational, regulatory, economic, and societal expectations.

To address this challenge, this study developed a dual contribution. The first one consists of the SERS framework itself, a stakeholder-oriented assessment framework that structures key non-functional dimensions and associated evaluation criteria. The framework was derived through an SLR and subsequently validated through expert consensus

using the fuzzy Delphi method. The second artefact consists of a multi-layer architecture integrating distributed ledger technologies, IoT, and Edge/Fog/Cloud computing. The architecture was designed using the SERS framework and evaluated through the Fuzzy-ANP approach.

The healthcare domain was used as a proof-of-concept because it represents a highly regulated and stakeholder-intensive environment where concerns related to security, privacy, resilience, and operational efficiency are particularly critical. The evaluation results indicate that the proposed architecture performs especially well in terms of security and resiliency, while also highlighting opportunities for further improvements regarding efficiency and sustainability.

From a practical perspective, the SERS framework provides decision-makers, enterprise architects, system designers, and technology adopters with a structured mechanism for evaluating and designing distributed ledger-based solutions. By explicitly incorporating SERS values into the assessment process, the framework supports informed technology adoption and architectural decision-making. Organizations can use the framework to identify potential trade-offs between stakeholder expectations and technical design choices, assess the suitability of blockchain-based solutions, and guide the integration of distributed ledger technologies with complementary technologies such as IoT and Edge/Fog/Cloud computing.

Although validated within a healthcare context, the SERS framework is not healthcare-specific. The framework and associated design principles can support the development and evaluation of distributed ledger systems across a broad range of domains, including supply chain management, smart cities, industrial IoT, digital government, and financial services. Future research should investigate the applicability of the framework in these contexts while further exploring mechanisms to improve the efficiency and sustainability of distributed ledger-based infrastructures.

Acknowledgement

Fatemeh Esmaeilnezhadtanha is supported by the National Interest Doctorate Program in Blockchain and Distributed Ledger Technology, Italian Ministry of University and Research.

Notes

1. <https://sqmagazine.co.uk/internet-of-things-statistics/>.
2. <https://data.mendeley.com/datasets/wmdhhs8vs2/.1>

Author contributions

CRedit: **Fatemeh Esmaeilnezhadtanha**: Conceptualization, Data curation, Formal analysis, Methodology, Supervision, Validation, Writing – original draft, Writing – review & editing; **Aliakbar Hasani**: Conceptualization, Data curation, Validation, Writing – original draft; **Luca Spalazzi**: Conceptualization, Data curation, Investigation, Methodology, Project administration, Supervision, Writing – original draft, Writing – review & editing; **Yves Wautelet**: Conceptualization, Methodology, Project administration, Supervision, Writing – original draft, Writing – review & editing.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Declaration of generative AI in scientific writing

During the preparation of this work, the authors used 'Grammarly' and ChatGPT in order to improve readability and language. After using these tools/services, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

ORCID

Fatemeh Esmailnezhadtanha  <https://orcid.org/0009-0005-3833-6823>

Yves Wautelet  <http://orcid.org/0000-0002-6560-9787>

References

- Abbasi, M., Prieto, J., Shahraki, A., & Corchado, J. M. (2023). Industrial data monetization: A block-chain-based industrial IoT data trading system. *Internet of Things*, 24, 100959. <https://doi.org/10.1016/j.iot.2023.100959>
- Acharya, V., Eswararao Yerrapati, A., & Prakash, N. (2019). *Oracle blockchain quick start guide: A practical approach to implementing blockchain in your enterprise*. Packt Publishing, Limited.
- Adere, E. M. (2022). Blockchain in healthcare and IoT: A systematic literature review. *Array*, 14, 100139. <https://doi.org/10.1016/j.array.2022.100139>
- Ahmad, I., Abdullah, S., & Ahmed, A. (2022). IoT-fog-based healthcare 4.0 system using blockchain technology. *The Journal of Supercomputing*, 79, 3999–4020. <https://doi.org/10.1007/s11227-022-04788-7>
- Al-Matari, N. Y., Zahary, A. T., & Al-Shargabi, A. A. (2024). A survey on advancements in blockchain-enabled spectrum access security for 6G cognitive radio IoT networks. *Scientific Reports*, 14(1), 30990. <https://doi.org/10.1038/s41598-024-82126-y>
- Alt, R., & Gräser, M. (2025). Distributed ledger technology. *Electronic Markets*, 35(1), 53. <https://doi.org/10.1007/s12525-025-00784-w>
- Ambriola, V., & Tortora, G. (Eds.). (1993). *Advances in Software Engineering and Knowledge Engineering* (Vol. 2). World Scientific. <https://doi.org/10.1142/2207>
- Andrew, J., Isravel, D. P., Sagayam, K. M., Bhushan, B., Sei, Y., & Eunice, J. (2023). Blockchain for health-care systems: Architecture, security challenges, trends and future directions. *Journal of Network and Computer Applications*, 215, 103633–103633. <https://doi.org/10.1016/j.jnca.2023.103633>
- Antonio, G., Camilo, G. F., Airam, L., Potop-Butucaru, M., Dias, M., Elias, M., & Henrique, L. (2024). A survey on blockchain scalability: From hardware to layer-two protocols. *IEEE Communications Surveys and Tutorials*, 1–1. <https://doi.org/10.1109/comst.2024.3376252>
- Bauer, I., Ziolkowski, R., Hacker, J., & Schwabe, G. (2023). Why blockchain: A socio-technical perspective on the motives of business consortia members to engage with blockchain technology. *Distributed Ledger Technologies: Research and Practice*, 2(2), 1–27. <https://doi.org/10.1145/3573893>
- Birje, M. N., Goudar, R. H., Rakshitha, C. M., & Tapale, M. T. (2022). A review on layered architecture and application domains of blockchain technology. In *2022 International Conference on Electrical, Computer and Energy Technologies (ICECET)* (pp. 1–5). IEEE. <https://doi.org/10.1109/ICECET55527.2022.9872729>
- Burhan, M., Rehman, R., Khan, B., Kim, B.-S., & Elements, I. (2018). Layered architectures and security issues: A comprehensive survey. *Sensors (Basel, Switzerland)*, 18(9), 2796. <https://doi.org/10.3390/s18092796>

- Eren, H., Karaduman, Ö., & Gençoğlu, M. T. (2025). Security challenges and performance trade-offs in on-chain and off-chain blockchain storage: A comprehensive review. *Applied Sciences*, 15(6), 3225. <https://doi.org/10.3390/app15063225>
- Esmailnezhadthanha, F., Spalazzi, L., Del Bene, L., & Wautelet, Y. (2025). A systematic literature review on distributed ledger technologies in healthcare: Applications, challenges, and future directions. *Information and Software Technology*, 188, 107894. <https://doi.org/10.1016/j.infsof.2025.107894>
- Firouzi, F., Farahani, B., & Marinšek, A. (2021). The convergence and interplay of edge, fog, and cloud in the AI-driven Internet of Things (IoT). *Information Systems*, 107, 101840. <https://doi.org/10.1016/j.is.2021.101840>
- Gangwal, A., Gangavalli, H. R., & Thirupathi, A. (2023). A survey of layer-two blockchain protocols. *Journal of Network and Computer Applications*, 209, 103539. <https://doi.org/10.1016/j.jnca.2022.103539>
- Gardas, B. B., Heidari, A., Navimipour, N. J., & Unal, M. (2022). A Fuzzy-based method for objects selection in blockchain-enabled edge-IoT platforms using a hybrid multi-criteria decision-making model. *Applied Sciences*, 12(17), 8906. <https://doi.org/10.3390/app12178906>
- Gu, L., Cui, M., Xu, L., & Xu, X. (2023). Collaborative offloading method for digital twin empowered cloud edge computing on internet of vehicles. *Tsinghua Science and Technology*, 28(3), 433–451. <https://doi.org/10.26599/tst.2022.9010006>
- Hasani, A., & Haseli, G. (2024). Digital transformation technologies for sustainable supply chain. *Decision Support Systems for Sustainable Computing*, 149–168. <https://doi.org/10.1016/b978-0-443-23597-9.00007-x>
- Hasani, A., Haseli, G., & Deveci, M. (2025). Analyzing operational risks of digital supply chain transformation using hybrid ISM-MICMAC method. *OPSEARCH*, 62, 583–607. <https://doi.org/10.1007/s12597-024-00792-y>
- Hevner, A., March, S., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75–105. <https://doi.org/10.2307/25148625>
- Ishikawa, A., Amagasa, M., Shiga, T., Tomizawa, G., Tatsuta, R., & Mieno, H. (1993). The max-min Delphi method and fuzzy Delphi method via fuzzy integration. *Fuzzy Sets and Systems*, 55(3), 241–253. [https://doi.org/10.1016/0165-0114\(93\)90251-c](https://doi.org/10.1016/0165-0114(93)90251-c)
- Kruchten, P. (1995). Architecture blueprints—the “4 + 1” view model of software architecture, Tutorial Proceedings on TRI-Ada ‘91 Ada’s Role in Global Markets: Solutions for a Changing Complex World - TRI-Ada ‘95. <https://doi.org/10.1145/216591.216611>
- Maden, A. (2019). Suitability evaluation of blockchain-based systems using fuzzy ANP- a case study in a logistics company. In C. Kahraman, S. Cebi, S. Cevik Onar, B. Oztaysi, A. Tolga, & I. Sari (Eds.), *Intelligent and fuzzy techniques in big data analytics and decision making. INFUS 2019. Advances in intelligent systems and computing* (pp. 401–407). Springer. https://doi.org/10.1007/978-3-030-23756-1_50
- Muneeb, M., Ko, K.-M., & Park, Y.-H. (2021). A fog computing architecture with multi-layer for computing-intensive IoT applications. *Applied Sciences*, 11(24), 11585. <https://doi.org/10.3390/app112411585>
- Obaidat, M. A., Rawashdeh, M., Alja’afreh, M., Abouali, M., Thakur, K., & Karime, A. (2024). Exploring IoT and blockchain: A comprehensive survey on security, integration strategies, applications and future research directions. *Big Data and Cognitive Computing*, 8(12), 174–174. <https://doi.org/10.3390/bdcc8120174>
- Oliveira, E., da Rocha, A. R., Mattoso, M., & Delicato, F. C. (2022). Latency and energy-awareness in data stream processing for edge based IoT systems. *Journal of Grid Computing*, 20(3), 27. <https://doi.org/10.1007/s10723-022-09611-4>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., & McGuinness, L. A. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *British Medical Journal*, 372, 71. <https://doi.org/10.1136/bmj.n71>
- Perry, D. E., & Wolf, A. L. (1992). Foundations for the study of software architecture. *ACM SIGSOFT Software Engineering Notes*, 17(4), 40–52. <https://doi.org/10.1145/141874.141884>

- Ramachandran, M. (2023). S3EF-HBCAs: Secure and sustainable software engineering framework for healthcare blockchain applications. *Blockchain in Healthcare Today*, 6(2), 286. <https://doi.org/10.30953/bhty.v6.286>
- Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, 3(5), 637–646. <https://doi.org/10.1109/jiot.2016.2579198>
- Tabatabaei, M. H., Vitenberg, R., & Veeraragavan, N. R. (2023). Understanding blockchain: Definitions, architecture, design, and system comparison. *Computer Science Review*, 50, 100575. <https://doi.org/10.1016/j.cosrev.2023.100575>
- Vingerhoets, A. S., Heng, S., & Wautelet, Y. (2021). Using i* and UML for blockchain oriented software engineering: Strengths, weaknesses, lacks and complementarity. *Complex Systems Informatics and Modeling Quarterly*, 26(26), 26–45. <https://doi.org/10.7250/csimq.2021-26.02>
- Wautelet, Y., & Rouget, X. (2025). Circulise, a model-driven framework to build and align socio-technical systems for the twin transition: Fanyatu's case of sustainability in reforestation. *Expert Systems with Applications*, 262, 125664. <https://doi.org/10.1016/j.eswa.2024.125664>

Appendix 1

Likert spectrum	Fuzzy scale		
Quite important	0.6	8.0	1
Very important	0.4	6.0	8.0
Relatively important	0.2	4.0	6.0
Poor importance	0	2.0	4.0
Equal importance	0	0	2.0

Table A.1. Linguistic variable transformation to an equivalent fuzzy number in the Delphi method

Linguistic Scale	Values interest	TFN Scale	TFN inverse Scale
Equally important	1	(1,1,1)	(1,1,1)
A little more important	3	(1,3,5)	(1/5,1/3,1)
More important	5	(3,5,7)	(1/7,1/5,1/3)
Very important	7	(5,7,9)	(1/9,1/7,1/5)
The most important	9	(7,9,11)	(1/11,1/9,1/7)

Table A.2. Triangular fuzzy number (TFN) scale and linguistic variables scale conversion

Questionare:

Survey for Research Study

We aim to design a healthcare data management information system leveraging IoT and blockchain technologies. To ensure the robustness of this system, we require an assessment performance framework. This framework will be utilized to evaluate the designed system's performance. To do so, we take two steps:

First step – having an assessment framework.

Second step – using the framework obtained in the first step to evaluate the designed architecture

This survey is related to the first step

Here we propose an assessment framework and we ask you to kindly review and evaluate such framework. The developed assessment framework is structured around four primary criteria: security, efficiency, resiliency, and sustainability. Each primary criterion encompasses various sub-criteria that serve as measurement scales.

The importance of each criterion will be determined based on its sub-criteria. In your evaluation, you focus on the importance of each criterion based on its respective sub-criteria. This evaluation will determine the necessity and relevance of each component.

Furthermore, we welcome suggestions for additional criteria and sub-criteria, including their importance levels, to enhance our assessment system. Based on your expert opinion, we will refine and finalize the assessment framework.

When you submit this form, it will not automatically collect your details like name and email address unless you provide it yourself.

1. Index evaluation: **Security**

Here is the definition of each subcriterion that we considered for the assessment framework.

Defended: The ability to respond to various cyber-physical attacks.

Protected: Having the proper level of protection, having an efficient active response to threats, and being safe from danger and harm.

Strengthened: The system should facilitate the strengthening of security, also from the point of view of organizational processes

Tested: The system should be tested under real-life conditions

	Not at all important	Somewhat unimportant	Neutral	Somewhat important	Extremely important
Defended	☐	☐	☐	☐	☐
Protected	☐	☐	☐	☐	☐
Strengthened	☐	☐	☐	☐	☐
Tested	☐	☐	☐	☐	☐

2. Index evaluation: **Efficiency**

Here is definition of each subcriterion that we considered for the assessment framework.

Accessible and Affordable

The ability to facilitate and make convenient access to the healthcare service for any category of people

Cost-effective: The ability to deliver optimal performance and benefits relative to its expenses.

Optimized: The ability to improve performance of healthcare services

Reliable: Considered as the reliability under various operational conditions.

	Not at all important	Somewhat unimportant	Neutral	Somewhat important	Extremely important
Accessible and affordable	☐	☐	☐	☐	☐
Cost-effective	☐	☐	☐	☐	☐
Optimized	☐	☐	☐	☐	☐
Reliable	☐	☐	☐	☐	☐

3. Index evaluation: **Resiliency**

Here is definition of each subcriterion that we considered for the assessment framework.

Recovery: The capability to quickly as well as efficiently return to normal status after a disruption occurrence.

Redundancy: Considered as incorporating backup resources to support primary systems under failure.

Resourcefulness: The ability to find quick and clever ways to manage a disruption.

Robustness: The ability to preserve key operations under disruption.

	Not at all important	Somewhat un important	Neutral	Somewhat important	Extremely important
Recovery	☐	☐	☐	☐	☐
Redundancy	☐	☐	☐	☐	☐
Resourcefulness	☐	☐	☐	☐	☐
Robustness	☐	☐	☐	☐	☐

4. Index evaluation: **Sustainability**

Here is definition of each subcriterion that we considered for the assessment framework.

Focus on value-added core competencies

The capability that provides value within the healthcare service-providing system and enhances its competitive advantage and delivers superior services to its stakeholders.

Reduce resource usage: The optimization of the utilization of resources such as energy, water, materials, and other inputs in the operations of the healthcare system.

Reduce total operation costs

The strategic effort of minimizing the overall expenses associated with the functioning of the healthcare system.

Reduce wastes: The focus is on implementing measures to minimize the generation of unnecessary waste materials within the healthcare system such as medical waste.

	Not at all important	Somewhat un important	Neutral	Somewhat important	Extremely important
Focus on value-added core competencies	☐	☐	☐	☐	☐
Reduce resource usage	☐	☐	☐	☐	☐
Reduce the total operation cost	☐	☐	☐	☐	☐
Reduce wastes	☐	☐	☐	☐	☐

5. **Suggestions for introducing new criteria and/or sub-criteria and their importance:**

6. Full name

7. Affiliation

Submit