Ensuring Data Sovereignty in IoT Systems for Cognitively Impaired Seniors through Delegated Data Management

Hércules S. S. José[1]

[1]Departamento de Ciência e Tecnologia – Universidade Aberta (UAb)
Lisboa, Portugal

2202365@estudante.uab.pt

Abstract. *IoT technologies for seniors improve independence and well-being, but managing sensitive health data can be difficult for those with cognitive impairments. The existing PDS architecture lacks a formal delegation mechanism to enable third parties to manage data on behalf of users. Using the DSR approach, the study proposes a PDS-based delegated data management framework with a delegation-aware component that mediates access requests, enforces scoped and time-bounded authority, and records auditable decision trails. The expected contribution is a capacity-aware, sovereignty-aligned mechanism for secure delegation that preserves residual autonomy while reducing risks of misuse and exploitation.*

Keywords. *IoT, cognitive impairment, data sovereignty, GDPR compliance, Solid protocol, delegated consent, older adults, delegated data management*

1. Introduction

The Internet of Things (IoT) has experienced exponential growth across sectors, with healthcare emerging as a particularly transformative domain. According to [Singh et al. 2023], the global healthcare IoT market is projected to reach $446.52 billion by 2028, growing at a compound annual rate of 18.3% from 2023. This remarkable expansion is driven by increasing demands for solutions in remote patient monitoring, preventive care, and personalized health management. [Kelly et al. 2020] demonstrate that IoT-enabled healthcare systems are fundamentally changing patient care delivery models, allowing continuous monitoring outside traditional clinical settings. This shift has proven especially beneficial for aging populations, where remote monitoring can reduce hospitalization rates for chronic conditions by up to 40% [Testa et al. 2025]. Connected devices, wearables, and smart home systems enable tracking of activity levels, fall detection, medication management, and provision of real-time data to caregivers, significantly contributing to elderly healthcare [Matayong et al. 2025].

With the significant growth of the aging population, the number of individuals experiencing cognitive decline is also increasing. Neurodegenerative conditions, including Alzheimer's disease, vascular dementia, and Parkinson's disease, along with stroke-related sequelae and traumatic brain injuries, represent the primary causes of cognitive decline. These conditions compromise critical cognitive functions such as memory, language processing, reasoning, and decision-making capacity, thereby diminishing personal autonomy and reducing overall quality of life. IoT technologies offer valuable support through continuous monitoring of activities of daily living, fall detection, vital signs monitoring, medication adherence systems, and social engagement

tools [Salvi et al. 2025; Sheikhtaheri and Sabermahani 2022]. For physicians, IoT-based systems provide actionable insights and automated alerts to support clinical decision-making, while also alleviating caregivers' stress through real-time monitoring [Alexandru et al. 2024].

Despite their clinical and societal benefits, IoT-based systems raise substantial security and privacy challenges that directly affect their adoption, particularly when deployed for cognitively impaired seniors. IoT ecosystems are characterized by pervasive data collection, heterogeneous devices, and complex data flows across organizational boundaries, which increase the attack surface and risks of unauthorized access, data leakage, and secondary data use [Kumar et al. 2023]. For cognitively impaired seniors, these risks are amplified by diminished capacity to understand consent mechanisms and the implications of data sharing [Saka and Das 2025]. In response to these privacy concerns, Personal Data Stores (PDS) have emerged as a promising approach, acting as decentralized, user-controlled repositories that enforce granular access control, data portability, and transparent governance, thereby aligning with core principles of data protection regulations such as the GDPR [Pinto et al. 2024; Pinto and Prazeres 2025].

2. Research Problem

Current PDS implementations assume direct and unrestricted user access to their personal data, without formal mechanisms for delegated data governance. This is especially clear when a user, the primary data subject, cannot independently manage access control policies due to cognitive impairment, legal age, temporary incapacity, or organizational delegation needs, requiring someone else to manage their data on their behalf. Existing PDS frameworks, such as SoLiD [Sambra et al. 2016], rely on a “privacy self-management” model where the data subject is presumed to be a capable decision-maker with the ongoing ability to handle complex permission settings [Solove 2021; Waldman 2020], thus excluding multi-actor governance scenarios that demand limited and auditable delegation.

The challenge of adding delegation features into PDS architectures is not just an implementation detail but a fundamental design problem involving three interconnected technical gaps. First, an architectural gap: current PDS implementations lack the necessary components to support multi-actor data governance—specifically, delegation services to mediate access requests, policy engines to evaluate context-dependent permissions, and surrogate management interfaces to distinguish between principal and delegated authority [Čučko and Turkanović 2025]. Second, delegation model gap: existing access control models within PDS ecosystems do not provide formal mechanisms to translate delegation instruments—such as scoped authority, temporal constraints, revocability, and non-delegable rights—into executable digital policies [Schmid et al. 2024]. Third, auditability gap: PDS architectures lack comprehensive audit trail mechanisms capable of detecting delegation overreach—situations where delegates exceed their granted authority—and supporting post-hoc accountability review [Ghayvat et al. 2022].

These architectural gaps have significant implications for IoT-based health monitoring systems, where the continuous collection of data from heterogeneous IoT devices creates complex real-time data governance challenges. In healthcare contexts involving cognitively impaired seniors, the lack of delegation mechanisms in PDS

architectures leads to what [Köhler et al. 2024] describes as a "consent gap": systems either block access to essential health services or default to highly permissive settings, risking data exposure. Current proposals, such as Ubi-Care [Chen et al. 2024], attempt to address collaborative data management through decentralized storage, but they face the "consent paradox" [Ghayvat et al. 2022]: establishing delegation generally requires informed consent from the principal—impossible when the principal lacks decision-making capacity. The main challenge our study addresses is the lack of a PDS-based framework that offers formal, bounded, and auditable delegation principles, while maintaining decentralization and user sovereignty.

3. Research Objectives and Questions

Research Objective: *Design, prototype, and evaluate a delegation-aware extension to PDS-based IoT architecture that supports delegated data governance of health data with auditability for cognitively impaired seniors.*

General Research Question: *How can delegated data governance be incorporated into a PDS-based architecture so that designated surrogates (caregivers, families, physicians) can govern IoT health data on behalf of cognitively impaired seniors without exceeding defined authority boundaries?*

Main Hypothesis: *Extending a PDS-based IoT architecture with a formal delegation model — comprising scoped authorization and audit logging — produces a demonstrably functional and auditable mechanism for delegated data governance in IoT health scenarios that also prevents delegation overreach.*

This general question decomposes into three specific research questions (SRQs) corresponding to the three primary artifacts that will be produced:

SRQ1 (Delegation Model): *How can legal delegation instruments be translated into scoped, time-bounded, and revocable digital permissions within the framework?*

SRQ2 (Audit Mechanism): *Does the audit trail mechanism detect and log delegation overreach in a way that supports post-hoc accountability review?*

SRQ3 (Conceptual Architecture): *What architectural extensions are required to incorporate multi-actor delegated management into a PDS-based IoT architecture?*

4. State of the Art

Due to privacy concerns affecting the adoption of IoT systems – risk of unauthorized access, opacity of data flows across device vendors – some mitigation strategies have been proposed, including federated learning [Ghosh and Ghosh 2023], blockchain solutions [Sharma et al. 2023], and data anonymization techniques [Andrew et al. 2023]. Among these, PDS stands out as a particularly promising method [Pinto and Prazeres 2025], as it uniquely combines decentralized data control with standards-based authorization protocols. In particular, the SoLiD [Sambra et al. 2016] advances this vision by enabling user-centric data sovereignty through decentralized Personal Online Datastores (PODs) that give individuals granular, revocable control over their personal information. This approach enables fine-grained, revocable permissions that comply with data protection regulations, such as the principle of purpose limitation and the right to erasure [Hummel et al. 2021].

Existing PDS implementations exhibit systematic gaps when delegation involves users with capacity limitations. [Čučko and Turkanović 2025] demonstrate that Self-Sovereign Identity (SSI) systems, which underpin many PDS architectures, structurally assume autonomous credential management, thus excluding individuals who lack independent authentication capabilities. [Schmid et al. 2024] propose Rights Delegation Proxies within Solid dataspaces for enterprise scenarios, yet these mechanisms presuppose that delegators possess sufficient cognitive capacity to define scoped policies and validate delegated actions—a condition that is progressively undermined in dementia contexts. Healthcare-focused PDS frameworks such as Ubi-Care [Chen et al. 2024] and SHARIF [Ghayvat et al. 2022] enable collaborative data management between patients and caregivers through Solid-based authentication, but both encounter what [Ghayvat et al. 2022] explicitly terms the "consent paradox": establishing delegation requires informed consent from the senior, rendering the system inoperable for those in advanced cognitive decline. Emerging solutions, including AI-assisted consent mechanisms [Pinto et al. 2025] and formalized Verifiable Mandates [Čučko and Turkanović 2025], represent preliminary attempts to operationalize time-bounded delegation, yet none provide mechanisms to preserve residual autonomy while preventing surrogate overreach in continuous data governance contexts.

Currently, no PDS-based architecture integrates: (1) capacity-aware delegation that adapts to cognitive fluctuation, (2) risk-graduated authority enforcement distinguishing routine from high-stakes data access, and (3) auditable overreach detection mechanisms supporting post-hoc accountability review. This work addresses this gap by extending PDS-based architectures with a formal delegation model and audit-first design that operationalizes legal delegation instruments as scoped, time-bounded digital permissions.

5. Research Methodology

This work adopts the Design Science Research (DSR) methodology [Peffers et al. 2007], justified by three reasons: (1) the problem is essentially a design issue—no existing PDS architecture properly tackles delegated governance for reduced capacity; (2) solving it involves creating new artifacts that combine technical, legal, and normative requirements rather than testing existing theories; and (3) DSR allows for iterative refinement through cycles of design and evaluation, making it suitable for emerging fields where requirements develop through prototyping rather than being fully defined in advance.

Three primary artifacts will be designed and evaluated:

- **Artifact 1 – Formal Delegation Model (SRQ1):** Metamodel (UML/ontology) and policy schema translating legal delegation instruments (powers of attorney, guardianship, supported decision-making) into scoped, time-bounded, revocable digital permissions. Includes policy representation for encoding actors, rights/duties, scope (data types, actions, devices, purposes), temporal constraints, and revocation/suspension/break-glass conditions. **Evaluation:** Functional testing via 20-40 test cases derived from legal/ethical scenarios, comparing actual vs. expected authorization decisions.
- **Artifact 2 – Audit Logging Component (SRQ2):** Implementation integrated with PDS and the delegation component, capturing delegation lifecycle events, access requests, authorization decisions, break-glass activations, and errors with

mandatory fields (actor, role, principal, delegation ID, data category, action, decision, timestamp, context). **Evaluation:** Simulation-based evaluation generating controlled logs with both legitimate and overreach behaviors.

- **Artifact 3 – Conceptual Architecture (SRQ3):** Extension of PDS-based IoT systems with delegation-aware mechanisms (delegation service, policy decision/enforcement points, surrogate management, audit logging). **Evaluation**: Analytical architecture evaluation via checklist-based quality assessment (modularity, separation of concerns, security, auditability) and scenario-based walkthroughs tracing 10-15 usage scenarios (delegation setup, revocation, break-glass, multi-surrogate coordination) through architectural components.

5.1. Preliminary Design Concepts

In a preliminary design concept, we propose a delegation-aware component—a technical intermediary between cognitively impaired seniors and authorized representatives—that manages all data access decisions within a Solid POD (Figure 1). Unlike traditional systems that centralize control in institutional databases, this architecture keeps data custody with the user-controlled POD while adding safeguards against misuse through three main internal mechanisms.

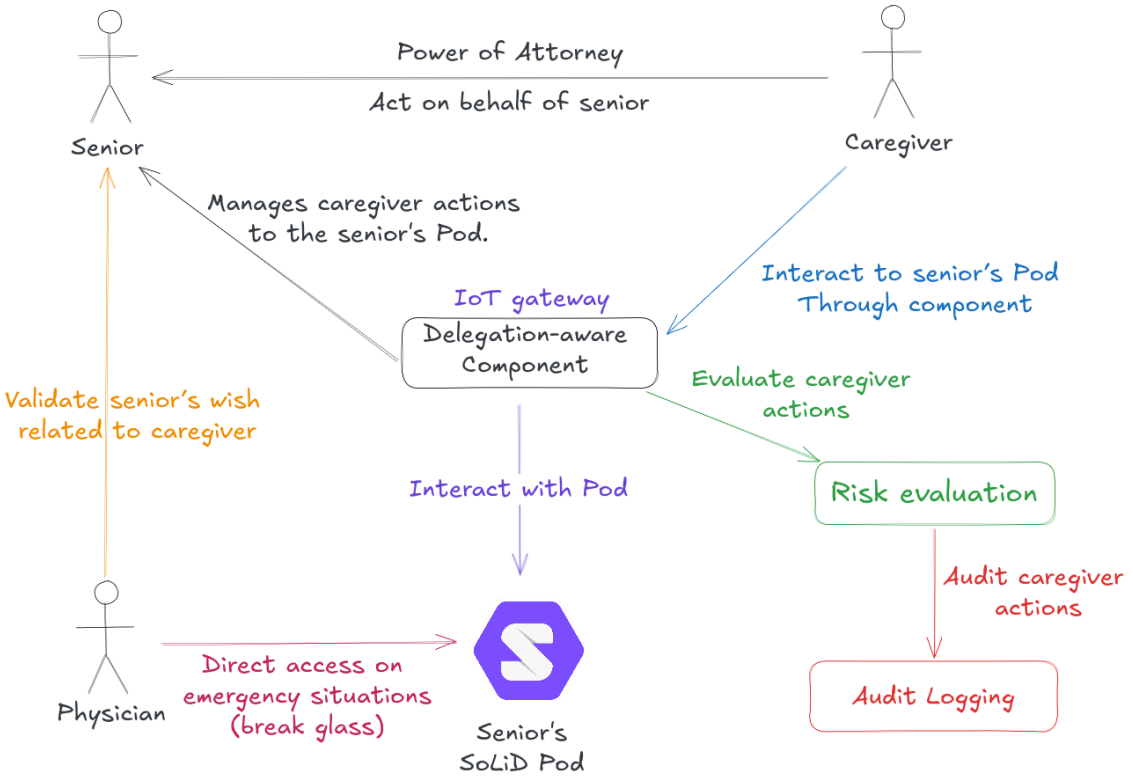

Figure 1. A delegated management framework proposal

- **Capacity-Aware Consent Mediation:** Distinguishes between access requests that seniors can meaningfully evaluate on their own and those that require proxy decision-making. Routes comprehensible low-risk requests directly to seniors with simplified explanations; escalates high-risk or complex requests to designated surrogates. Acknowledges that capacity varies across decision contexts rather than representing a global binary state.

- **Risk-Based Access Evaluation:** Incorporate ongoing risk assessments by evaluating requests based on data sensitivity, intended use, and recipient credentials. High-risk requests (e.g., granting broad permissions to new caregivers or sharing complete medical histories) require more thorough review and may need clinical verification, regardless of the assessed capacity.
- **Clinical Verification of Critical Delegations:** Requires physician confirmation when seniors establish or revoke power of attorney for data management, to verify that decisions reflect authentic preferences and adequate understanding. Furthermore, in an emergency, physicians have direct access to the seniors' pod in the caregiver's absence (break-glass).

The architecture employs standard SoLiD protocols for data storage and access control while extending authorization evaluation to incorporate delegation policies with temporal constraints, scope boundaries (data types, purposes, authorized actions), and revocation conditions. All delegation-related events are logged through audit logging mechanisms, with complete provenance chains that enable post-hoc reconstruction of authorization decisions and detection of boundary violations and overreach.

6. Expected Contributions

This work is expected to advance the state of the art in privacy-preserving healthcare IoT and software engineering by delivering a novel architecture component that operationalizes delegated data management for cognitively impaired seniors. The expected outcomes are structured around three primary deliverables, corresponding to our research questions:

- **Delegation Meta-Model and Engine (SRQ1):** A concrete policy schema to encode delegations derived from legal instruments (powers of attorney, guardianship, supported decision-making). The delegation engine will create, modify, and revoke active delegation policies, evaluate access requests in context, and enforce constraints (scope, time, revocation).
- **Audit Model and Logging Mechanism (SRQ2):** An implementation integrated with the PDS and delegation engine, defining event types and fields (delegation lifecycle events, access requests, authorization decisions, break-glass activations). This append-only and tamper-evident mechanism will support detection logic (query scripts or rule engine) to compare each access to the active delegation at that time, flagging potential overreach events.
- **Extended Conceptual Architecture (SRQ3):** A formal model capturing actors (principal, surrogate, affiliate), rights, duties, and scope (data types, actions, devices, purposes). This includes component, deployment, and data-flow diagrams that show the integration of PDS, the delegation service, policy decision/enforcement, surrogate management, and audit logging.

7. Conclusions and Next Steps

This work addresses an important gap in current PDS-based architectures: the lack of formal mechanisms to support delegated data governance for cognitively impaired seniors within IoT healthcare systems. While existing PDS implementations assume direct user

control, they often exclude individuals whose impaired cognitive capacity prevent them from managing their data independently. Our proposed delegation-aware extension to the PDS-based IoT architecture implements legal delegation tools—such as powers of attorney, guardianship, and supported decision-making—as scoped, time-limited, and revocable digital permissions. This approach helps bridge the gap between legal frameworks and technical implementation.

The research uses the DSR methodology to develop and evaluate three main artifacts: (1) a formal delegation model that transforms legal constructs into executable authorization policies, (2) an audit logging system that enables post-hoc accountability review and detection of overreach, and (3) an expanded conceptual architecture that integrates delegation services, policy enforcement, and surrogate management within PDS-based IoT systems. By combining capacity-aware consent mediation, risk-based access evaluation, and clinical verification mechanisms, the framework preserves residual autonomy while reducing the risk of exploitation and overreach.

Current work has completed the literature review and transitioned to the next phase of the research, which focuses on specifying and implementing the three primary artifacts and their evaluation strategies. For SRQ1, the delegation metamodel and engine will be refined and validated through scenario-based test cases derived from legal and ethical delegation situations. For SRQ2, the audit model and logging mechanism will be integrated into a proof-of-concept prototype and assessed via simulation logs to detect and flag delegation overreach. For SRQ3, the extended conceptual architecture will be consolidated and subjected to checklist-based quality assessment and walkthroughs of usage scenarios.

Acknowledgements

Special thanks to my advisors, Prof. Hugo Paredes (UTAD/INESCTEC), Prof. Luis Barbosa (UTAD/INESCTEC), and Prof. Nuno Rodrigues (IPCA/INESCTEC), for their support in continuing this work.

References

Alexandru, A., Ianculescu, M. and Paraschiv, E. A. (2024). Harnessing the Capabilities of IoHT-Based Remote Monitoring Systems for Decision Making in Elderly Healthcare. In: Balas, V. E.; Dzemyda, G.; Belciug, S.; Kacprzyk, J.[Eds.]. . *Decision Making and Decision Support in the Information Era: Dedicated to Academician Florin Filip*. Cham: Springer Nature Switzerland. p. 147–184.

Chen, H., Zhou, T. and Wu, B. (6 oct 2024). Ubi-Care: An Elderly Life Support Healthcare Framework Based on Ubiquitous Personal Online Data Stores. In *2024 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. . IEEE. https://ieeexplore.ieee.org/document/10831632/, [accessed on Jan 26].

Čučko, Š. and Turkanović, M. (2025). A Novel Model for Authority and Access Delegation Utilizing Self-Sovereign Identity and Verifiable Credentials. *IEEE Access*, v. 13, p. 115102–115134.

Ghayvat, H., Sharma, M., Gope, P. and Sharma, P. K. (aug 2022). SHARIF: Solid Pod-Based Secured Healthcare Information Storage and Exchange Solution in Internet of Things. *IEEE Transactions on Industrial Informatics*, v. 18, n. 8, p. 5609–5618.

Kelly, J. T., Campbell, K. L., Gong, E. and Scuffham, P. (10 nov 2020). The Internet of Things: Impact and Implications for Health Care Delivery. *Journal of Medical Internet Research*, v. 22, n. 11, p. e20135.

Kumar, M., Kumar, A., Verma, S., et al. (jan 2023). Healthcare Internet of Things (H-IoT): Current Trends, Future Prospects, Applications, Challenges, and Security Issues. *Electronics*, v. 12, n. 9, p. 2050.

Matayong, S., Jetwanna, K. W., Choksuchat, C., et al. (1 mar 2025). IoT-based systems and applications for elderly healthcare: a systematic review. *Universal Access in the Information Society*, v. 24, n. 1, p. 99–125.

Pinto, G. P., Donta, P. K., Dustdar, S. and Prazeres, C. (jan 2024). A Systematic Review on Privacy-Aware IoT Personal Data Stores. *Sensors*, v. 24, n. 7, p. 2197.

Pinto, G. P. and Prazeres, C. (jun 2025). Data Privacy in the Internet of Things: A Perspective of Personal Data Store-Based Approaches. *Journal of Cybersecurity and Privacy*, v. 5, n. 2, p. 25.

Pinto, G. P., Sousa, N. R., Da Silva, C. N., et al. (1 nov 2025). Enhancing IoT data privacy: AI-assisted consent mechanism in a PDS-based solution. *Internet of Things*, v. 34, p. 101807.

Saka, S. and Das, S. (25 apr 2025). "Watch My Health, Not My Data": Understanding Perceptions, Barriers, Emotional Impact, & Coping Strategies Pertaining to IoT Privacy and Security in Health Monitoring for Older Adults. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. , CHI '25. Association for Computing Machinery. https://dl.acm.org/doi/10.1145/3706598.3714019, [accessed on Jan 30].

Salvi, S., Garg, L. and Gurupur, V. (22 aug 2025). Stage-Wise IoT Solutions for Alzheimer's Disease: A Systematic Review of Detection, Monitoring, and Assistive Technologies. *Sensors*, v. 25, n. 17.

Sambra, A. V., Mansour, E., Hawke, S., et al. (2016). Solid: a platform for decentralized social applications based on linked data. *MIT CSAIL & Qatar Computing Research Institute, Tech. Rep.*, v. 2016.

Schmid, S., Schraudner, D. and Harth, A. (2024). The Rights Delegation Proxy: An Approach for Delegations in the Solid Dataspace.

Sheikhtaheri, A. and Sabermahani, F. (2022). Applications and Outcomes of Internet of Things for Patients with Alzheimer's Disease/Dementia: A Scoping Review. *BioMed Research International*, v. 2022, n. 1, p. 6274185.

Singh, B., Lopez, D. and Ramadan, R. (1 sep 2023). Internet of things in Healthcare: a conventional literature review. *Health and Technology*, v. 13, n. 5, p. 699–719.

Testa, D., Iborra, V., Dutech, M., et al. (10 sep 2025). Impact of a Home-Based Remote Patient Monitoring System on Hospitalizations and Emergency Department Visits of Older Adults With Polypathology: Multicenter Retrospective Observational Study. *Journal of Medical Internet Research*, v. 27, n. 1, p. e64989.