The Evolution Towards Decentralized and Privacy-Oriented Integration: Challenges and a New Perspective

Valdemar Vicente Graciano Neto[1], Rafael Z. Frantz[2]

[1]Instituto de Informática
Universidade Federal de Goiás (UFG)
Goiânia – GO – Brasil

[2]Unijuí University
Ijuí - RS - Brasil

valdemarneto@ufg.br, rzfrantz@unijui.edu.br

Abstract: *The integration of Information Systems (ISs) has expanded beyond single organizations to multi-organizational ecosystems, raising critical security and privacy challenges. Traditional centralized models, often controlled by BigTechs, create risks such as data misuse and vendor dependency. This paper explores decentralized integration as a solution, emphasizing privacy, security, and technological sovereignty. We highlight key challenges, including scalability, efficiency, and the adoption of Trusted Execution Environments (TEEs). To advance this field, we propose a Grand Challenge for IS: the development of privacy-oriented decentralized integration solutions.*

Palavras-chave*: decentralized systems, security, decentralized system integration.*

1. What is your idea, vision, or reflection on the challenges in Information Systems in Brazil for the next 10 years?

Information Systems (ISs) must interoperate to enhance functionalities and enable cross-domain integration. Traditionally, the researchers tackling the research field known as Enterprise Application Integration (EAI) and the practitioners of EAI in companies addressed the integration of systems within the same organization with little or no concern for security and data privacy. Nowadays, application integration activity inherently transcends a company's systems (and boundaries), requiring data exchange between systems from different organizations. In smart cities, for instance, integration extends beyond a single company, involving public and private systems. Therefore, integration moves beyond connecting systems within a "single-organization" ecosystem and demands connecting systems within a "multi-organizational" context in which systems from different organizations not only have to share data, but have functional dependencies. All these systems contain regular and sensitive data that has to be shared as well as functionalities that can be reused to support the business processes in companies.

In this context, challenges arise, such as creating an environment where data owners feel comfortable sharing their data. This requires security and privacy guarantees. The “piece of software” that connects these systems is what we technically call a decentralized integration solution supported by privacy enhancing technologies, through which data is securely processed and flows from one system and organization to another. The entity managing the integration solution must not have access to or filter such data, which is why these solutions need to be designed and run on a new model, a decentralized model. That is the challenge! How can we develop and implement these integration solutions? The challenge is related to (i) the high costs (particularly in effort and time) to establish such integrations and (ii) the nature of the technologies often used to integrate, which are majorly proprietary and provided by BigTechs (such as Google or Meta). As a consequence, current integrations (called centralized - In this context, centralization refers not to a single point of failure as a server, but to who has the control of the integration solution), suffering from the typical problems that arise from this fact, including data leaks and misuse (see cases like Cambridge Analytics and Facebook, where companies exploited user data in an unethical manner and had the potential to use it to manipulate public opinion; this was one of the biggest data privacy scandals in history, involving the misuse of information from millions of Facebook users for political purposes), privacy and security issues, and dependency or technological fragility problems, making Brazilian governments and enterprises dependent on BigTechs. Thus, we propose a new perspective on integration: a decentralized integration of information systems and its secure execution using emerging trusted hardware environments. This concept extends beyond traditional interoperability and aims to facilitate security, privacy, and self-sufficient interactions between systems and technolo- gies in contexts such as in smart cities [Graciano Neto and Kassab 2023].

2. Why is it critical for the community to direct efforts toward overcoming it?

Integration is needed to interoperate information systems. While interoperability ensures that systems can understand and process shared information across different levels, syntactic, semantic, technical, and organizational, integration is about creating the physical and technical pathways that enable interoperability to happen [França et al. 2024]. In other words, integration is the foundation upon which interoperability is built. Traditional EAI integration has long been a research focus [Hohpe and Woolf 2004], but the real challenge today lies in integrating systems from distinct organizations while ensuring, from a technical perspective, data privacy and security. While full interoperability has been pursued between 2016 and 2026 at multiple levels [Maciel et al. 2017], the next challenge is **endowing integration solutions with privacy and security guarantees**. To achieve this, we must explore new strategies, such as decentralized models and emerging technologies.

A **decentralized** integration seeks to give organizations control over their data while reducing dependency on a third-party. One approach gaining traction to endow security and privacy at execution time is the use of Trusted Execution Environments (TEEs) [Schuch et al. 2024], which allows software engineers to create secure en- claves where sensitive data is processed without exposing the data. TEEs like Intel SGX and

ARM Morello Boards enhance security by isolating sensitive computations. Hence, it is a critical advance in that area because it comprises (i) data privacy and security, a current important concern, and (ii) this also promotes the Brazilian technological sovereignty.

3. What are the risks if we fail to make progress in addressing it?

The lack of progress in decentralized integration may limit national competitiveness and technological sovereignty in integration solutions.

4. What other problems, areas, fields of knowledge, actions, initiatives, technolo- gies, etc., are related to this challenge?

This challenge is linked to several other challenges previously proposed by the community that still require advancements: Smart Cities, Systems-of-Information Systems, Full Interoperability, and the Open World [Araujo et al. 2017].

5. Final Remarks

Decentralized integration is a crucial challenge for information systems, requiring new methods to ensure security and sovereignty. The research agenda ahead must focus on developing technically feasible, socially impactful, and high-quality solutions while ensuring that the scientific apparatus supports the development of decentralized integration frameworks. By advancing these efforts, we can lay the foundation for a future where integration is democratized, independent from BigTech dominance, and truly aligned with the needs of an open, interconnected and secure world.

Acknowledgments

As required by the SBC Code of Conduct, we explicitly declare that ChatGPT (version 4-turbo) was used to write parts of this work. We are aware that the use of such tool does not exempt the authors from responsibility for all of their content, but we clarify that we curated the content and shaped it to the final version, besides writing most of it entirely from our hands and based on our experience on the subject. This research is partially funded by the Co-ordination for the Brazilian Improvement of Higher Education Personnel (CAPES) and the Brazilian National Council for Scientific and Technological Development (CNPq) under the following project grants 309425/2023-9, 402915/2023-2.

Referências

Araujo, R., Maciel, R., and Boscarioli, C. (2017). Grand Challenges in Information Systems for the Next 10 years. Brazilian Computer Society, Porto Alegre, Brazil. 1st Edition. 184 p.

Franca, A. G., Frantz, R. Z., and Neto, V. V. G. (2024). Unveiling a process for the establishment of interoperability links between software-intensive information systems. In Proceedings of the 20th Brazilian Symposium on Information Systems (SBSI), pages 1–10. ACM.

Graciano Neto, V. V. and Kassab, M. (2023). What Every Engineer Should Know About Smart Cities. CRC Press - Taylor & Francis. 1st Edition. 254 p.

Hohpe, G. and Woolf, B. (2004). Enterprise integration patterns: Designing, building, and de- ploying messaging solutions. Addison-Wesley Professional. 1st Edition. 736 p.

Maciel, R. S. P., David, J. M. N., Claro, D. B., and Braga, R. (2017). Grand Research Challenges in IS in Brazil, chapter “Full interoperability: Challenges and opportunities for future information systems”, pages 107–118. Brazilian Computer Society.

Schuch, R., Frantz, R. Z., Bocanegra, J., Roos-Frantz, F., Sawicki, S., and Molina-Jime´nez, C. (2024). Digital services integration in smart cities: a trusted execution environment based solution. In 27th Iberoamerican Conference on Software Engineering (CIbSE), pages 437– 438.