Enhancing Trust in Inter-Organisational Data Sharing: Levels of Assurance for Data Trustworthiness

Florian Zimmer[1][a], Janosch Haber[2][b] and Mayuko Kaneko[3][c]
[1]*Industrial Manufacturing, Fraunhofer ISST, Dortmund, Germany*
[2]*Fujitsu Research of Europe, Slough, U.K.*
[3]*Data & Security Research Laboratory, Fujitsu Limited, Kanagawa, Japan*
fl

Keywords: Data Trustworthiness, Levels of Assurance, Inter-Organisational Data Sharing, Trust, Data Spaces, Design Science Research.

Abstract: With data increasingly acknowledged as a valuable asset, much effort has been put into investigating inter-organisational data sharing to unlock the value of previously unused data. Hence, research has identified mutual trust between actors as essential prerequisite for successful data sharing activities. However, existing research oftentimes focuses on trust from a data provider perspective only. Our work, therefore, highlights the unbalanced view of trust and addresses trust barriers from a data consumer perspective. Investigating trust on a data level, i.e. the assessment and assurance of data trustworthiness, we found that existing solutions focused on data trustworthiness do not meet the domain requirements of inter-organisational data sharing. This paper addresses this shortcoming by proposing a new artifact called Levels of Assurance for Data Trustworthiness (Data LoA) based on a design science research approach. Data LoA provides an overarching, standardised framework to assure data trustworthiness in inter-organisational data sharing. Our research suggests that the adoption of this artifact would lead to an increase of data consumer trust. Still, being a first iteration artifact, Data LoA requires further design efforts before it can be deployed.

1 INTRODUCTION

The increasing adoption of information-driven technology across industries and its integration in nearly every aspect of life highlights the ever-growing importance of data. Data is considered a central driver in the acceleration of digital transformation and has been acknowledged as an essential asset for innovation and growth (Otto et al., 2022). As a result, inter-organisational data sharing has recently gained much attention in academia and industry, aiming to unlock the full potential of previously unused and underutilised data (Tocco and Lafaye, 2022).

However, organisations are often hesitant when engaging in data sharing activities, with a lack of trust and transparency mentioned as one of the most fundamental barriers (Jussen et al., 2023). The main reason for the lack of trust mentioned is challenges to *data sovereignty*, i.e. the concern of data providers to lose control over their data once shared with other organisations (von Scherenberg et al., 2024). *Data spaces* have emerged to overcome these concerns (Otto et al., 2022). However, the issue of trust here is predominantly considered from the perspective of the data provider. We found that current approaches often aim at preventing a loss of sensitive information or improving data security (Huber et al., 2022), but rarely mention the data consumers' risks and their need for trust in data providers and the data made available by them (Otto et al., 2022; Tocco and Lafaye, 2022).

Contrarily, data consumers are often referred to as *risk owners*, facing potential risks from data providers' insufficient measures to ensure data integrity (ISO and IEC, 2022). Because data is becoming crucial for (automated) decision making (Faheem Zafar et al., 2017), leveraging (un-)intentionally modified, incomplete, or compromised data exposes data consumers to potentially severe consequences from financial losses to human harm (Lim et al., 2012; Jaigirdar et al., 2019). Still, data consumers usually have no other option than to trust data providers, as trust for data itself cannot be established otherwise (Alhaqbani

[a] https://orcid.org/0009-0002-8060-7162
[b] https://orcid.org/0000-0001-5494-9770
[c] https://orcid.org/0000-0001-9873-2557

Zimmer, F., Haber, J., Kaneko and M.
Enhancing Trust in Inter-Organisational Data Sharing: Levels of Assurance for Data Trustworthiness.
DOI: 10.5220/0013461800003967
In *Proceedings of the 14th International Conference on Data Science, Technology and Applications (DATA 2025)*, pages 339-346
ISBN: 978-989-758-758-0; ISSN: 2184-285X

and Fidge, 2009).

In this paper, we argue that trust in inter-organisational data sharing should not be limited to the organisational level but must also encompass the trustworthiness of the data itself. Following a *design science research* (DSR) approach, we review existing literature on data trustworthiness. We systematically identify overarching design requirements for existing solutions and identify implications and challenges of establishing and assuring data trustworthiness in complex data sharing scenarios. Based on the identified problem and solution spaces, we aim to address the shortcomings of existing artifacts by introducing the concept of *Levels of Assurance for Data Trustworthiness*, or *Data LoA*, a novel framework for enhancing trust and transparency among data providers and consumers. In its first iteration, we develop a foundational model that outlines key actors and their interactions and present a *proof of concept* (PoC) implementation which demonstrates our concept. Our main contributions include:

(i) Compiled design knowledge, identifying existing work and mapping the problem and solution space

(ii) A novel Data LoA artifact aimed at enhancing data consumer trust in data sharing scenarios

The remainder is structured as follows: In Section 2 we touch on related work. Section 3 outlines the research methodology. Section 4 presents the derived design knowledge and proposes the concept of Data LoA. In Section 5, we discuss implications and limitations, and future work. Section 6 concludes the paper.

2 RELATED WORK

2.1 Data Trustworthiness

The trustworthiness of data has been extensively studied across various domains and applications such as healthcare, defence, traffic control, and manufacturing (Gomez et al., 2009). It is usually described as the possibility to ascertain the correctness of data provided by a data source (Haron et al., 2017). Yet, a high degree of context and domain dependency so far have prevented the formulation of a generally accepted notion of data trustworthiness (Bertino, 2015; Xu and MacAskill, 2023). Circumnavigating a holistic definition, literature oftentimes mentions specific dimensions of data trustworthiness, most commonly data quality, availability, security, and compatibility - each of which concerned with several different aspects themselves (Xu and MacAskill, 2023).

Previous work has produced a range of different artifacts to assure, measure, and define individual aspects of data trustworthiness. For instance, (Ormazabal et al., 2024) present a trust assessment canvas to gauge the trustworthiness of publicly available medical data. (Foidl and Felderer, 2023) present a trust score model capable of measuring the trustworthiness of industrial IoT data sources. And (Leteane and Ayalew, 2024) propose a trust-enhancing framework for data traceability in the context of food supply chains.

Some researchers argue that the variety of approaches and diversity of definitions prevents the development of an overarching, comprehensive solution to assure data trustworthiness (Bertino, 2015; Ebrahimi et al., 2022). Therefore, (Haron et al., 2017) argue that a combination of different techniques will be required to fully meet the trust-related requirements of data consumers.

2.2 Levels of Assurance

Levels of Assurance (LoA) refer to the degree of confidence that can be assigned to some entity, process, or system acting or operating as claimed (ISO and IEC, 2013). LoAs are an assurance technique used to evaluate and grade complex scenarios, simplifying and improving decision making and risk management (Nenadic et al., 2007). More formally, a *relying party* utilises provided LoA information to determine their level of confidence in the credibility of a *claimant's* claim. Usually, there is at least one other party involved, namely the *assurance provider*, which audits and assures the claimant's claim (Martínez-Ferrero and García-Sánchez, 2018; ISO and IEC, 2013). If there is no external assurance provider, claims are self-asserted.

LoAs are mainly used in the domain of identity validation, for example, in the ISO/IEC 29115[1] standard, the eIDAS regulation as proposed by the European Commission, or the NIST 800-63-A[2] guidelines. LoAs are defined risk-based, specifying dimensions of risk that must be addressed and mitigated to assure the credibility of a claim. Hence, the higher the perceived risk for the relying party, the higher the required level of confidence in the claim's validity, and thus the LoA should be (Martínez-Ferrero and García-Sánchez, 2018; ISO and IEC, 2013). A comprehensive LoA concept should guide the claimant on how to mitigate risks, while providing the relying party with assurances needed for informed decision making.

[1] https://iso.org/standard/45138.html

[2] https://pages.nist.gov/800-63-3/sp800-63a.html

Apart from that, eIDAS also aims to improve trust among adopters by assuring identification techniques and clearly defining liabilities to specify each party's responsibilities. Thus, eIDAS certifies commonly used identification techniques with different LoAs, providing standardised assurances to assess mutual trust and enabling interoperability in the heterogeneous identification techniques landscape of the EU (European Parliament, 2014).

3 METHODOLOGY

This paper aims to address the under-representation of trust-establishing means for data consumers in inter-organisational data sharing. To do so, we applied a rigorous DSR approach following (Peffers et al., 2007) to design a new *Levels of Assurance for Data Trustworthiness* (Data LoA) artifact that provides a framework for unifying and standardising the assurance of data trustworthiness. The goal of this artifact is twofold: First, it enables data consumers to assess the risks associated with utilising a shared data asset. Second, it equips data providers with standardised principles on how to establish different degrees of data trustworthiness assurances for the data they want to share. Together, these mechanisms are aimed at enhancing trust in inter-organisational data sharing and enabling interoperability among existing trust-assuring solutions.

We followed an objective-centred DSR approach building on existing data trustworthiness assuring artifacts. However, as previous artifacts were not necessarily developed under DSR, available design knowledge was limited. We therefore started by identifying the relevant problem and solution spaces, and identified the challenges, motivations, and goals addressed by existing artifacts. We did so by conducting a *structured literature review (SLR)* as described by (vom Brocke et al., 2015), deriving design knowledge by empirical means.

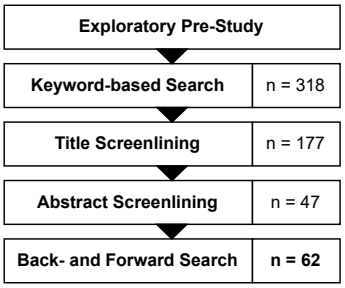

Figure 1: Conducted literature search approach.

Our SLR process, illustrated in Figure 1, resulted in 62 articles. The complete SLR process can be accessed for full transparency and reproducability at (Zimmer et al., 2025). We then empirically derived design knowledge for i) challenges and motivations in measuring and assuring data trustworthiness, and ii) common objectives and goals of existing artifacts. Formalising this information grounded the relevance of our artifact and focused our design efforts.

We continued our DSR objective-centred approach as pictured in Figure 2. We derived and selected a set of design objectives aligned with our overall goal of enhancing trust in inter-organisational data sharing, and used these objectives to guide the development of our artifact. During this stage, we noticed that the concept of LoAs for identity validation serves a very similar purpose in an adjacent domain and decided to use LoAs as inspiration for our artifact, adjusting our design goals accordingly.

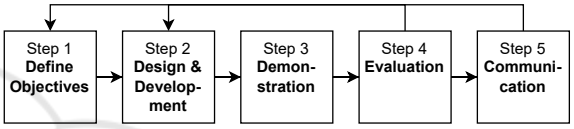

Figure 2: The objective-centred DSR approach following (Peffers et al., 2007) applied in this study.

Based on the identified design requirements, we then developed a first iteration of the Data LoA artifact. We mainly focused on defining central mechanisms, actors, and their relations to enable early evaluation and establish a sound foundation for future iterations. We evaluated our artifact by instantiating a PoC in the context of data spaces to investigate trust effects in our target domain. Conducting an experimental simulation allowed us to assess the technical feasibility of our concept and determine limitations and considerations for future work.

4 RESULTS

4.1 Design Knowledge & Grounding

An objective-centred DSR approach assumes a well-defined problem space (Peffers et al., 2007). As this was not the case, we conducted a SLR as described in Section 3 to extract and derive existing design knowledge. We compiled information on past artifact motivation and problem space definition from previous literature, identifying three main motivations and one key challenge for providing data trustworthiness assurance: i) mitigating undeterminable risks in data sharing, ii) unlocking the operational value of shared data assets, and iii) catering to an increasing demand

for trustworthy data. We also identified the complexity of assessing data trustworthiness as its main challenge. For brevity, we here only reference key literature. A full list of the analysed articles and derived clusters can be found in (Zimmer et al., 2025).

Improving trust in third-party data is crucial due to the **undeterminable risks** posed by using untrustworthy data. Data influences decision-making, impacting accuracy, reliability, and overall business success, highlighting the **operational value of data** (Haron et al., 2017; Karthik and Ananthanarayana, 2016). Thus, using untrustworthy data can negatively impact business success and lead to severe consequences (Jaigirdar et al., 2019). Therefore, ensuring data trustworthiness is driven by improved risk management and accountability, using only trustworthy data in high-risk environments, avoiding low-trustworthy data (Ardagna et al., 2021).

Furthermore, research suggests that there is an **increasing demand** for trustworthy data, mentioning an increased reliance on data for daily operations and the data-related risk attached to it as the primary cause (Bertino, 2015; Islam et al., 2025). Additionally, recent work emphasises the **increasing demand** for reliable data in *artificial intelligence* (AI) (Anjomshoaa et al., 2022). However, existing work also highlights that ensuring and assessing data trustworthiness is a challenging task. For instance, (Bertino, 2015) argues that addressing the different facets of data trustworthiness requires a complex combination of different approaches and techniques.

4.2 Design Objectives

To define our design objectives, we investigated the solution space populated by previous research. Based on our SLR, we identified 51 previous artifacts related to improving or assessing data trustworthiness, the majority of which are in the domain of IoT. Although the understanding of data trustworthiness differs in research, many artifacts do appear to have common goals, which we used to guide our design efforts. In total, we identified four central design objectives: i) improve data consumer trust in shared data assets, ii) reduce the risk of utilising third-party data assets, iii) decrease the complexity of assessing data trustworthiness, and iv) enable interoperability of existing approaches for assessing and assuring data trustworthiness.

Most of the identified goals are closely tied to the identified motivations and are interconnected with each other. The most important goal of existing solutions is to **enhance trust** in data, i.e., increasing a data consumer's confidence in the data they use (Alkhelaiwi and Grigoras, 2015). This is mirrored in research on inter-organisational data sharing, acknowledging trust as the most important factor for it to succeed (Tocco and Lafaye, 2022). Typically, artifacts enhance trust by increasing transparency and providing detailed information, such as data origin or provenance, or by providing a more simplified aggregated trust score (Foidl and Felderer, 2023; Leteane et al., 2024). Therefore, increasing transparency and **reducing trustworthiness assessment complexity** are also goals often mentioned. Moreover, tackling these issues also enables consumers to **mitigate risk** as they are enabled to make informed decisions, which ultimately allows them to avoid unsuitable data for use in potentially high-risk environments. This is in line with the domain of inter-organisational data sharing, as many different users with different backgrounds need to grow confident in the usage of third-party data while avoiding costly risks.

A key design objective missing in existing artifacts is **interoperability**. Most solutions address specific cases or domains like IoT. Still, existing solutions could play an important role in assuring data trustworthiness in the context of inter-organisational data sharing. Yet, there is no standardised trust model or overarching solution to enhance trustworthiness at the data level (Ebrahimi et al., 2022). As the identity LoA eIDAS was introduced for a similar reason, we believe that the current heterogeneous landscape of existing data trustworthiness artifacts would benefit from taking an analogous approach (European Parliament, 2014). Hence, the idea of LoA could be used to assess and assure the data trustworthiness based on existing solutions and measurements in place. Therefore, we adopt and apply this design goal inspired by the domain of LoAs for identity verification.

4.3 Artifact Description

Based on the formalised design knowledge and derived design goals, we developed a novel framework for data trustworthiness assurance in inter-organisational data sharing. The resulting artifact is an LoA-based assurance technique called *Levels of Assurance for Data Trustworthiness*, or short *Data LoA*. Similar to LoAs in other domains, we define Data LoA as follows: *Levels of Assurance for Data Trustworthiness refer to the degree of confidence that a data asset's underlying information can be trusted to be true.* In other words, Data LoA ensures the confidence a data consumer can put into a data asset's trustworthiness, considering the residual risks related to aspects not covered by the provided assurance. Within the Data LoA framework, we propose the fol-

lowing three actors and interactions as displayed in Figure 3.

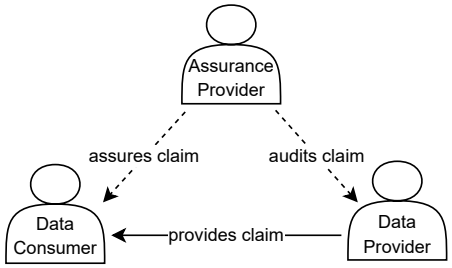

Figure 3: Abstract actor model of Data LoA.

Data Consumer. Using the terminology of LoAs for identity verification, the Data Consumer is the *relying party*. The Data Consumer is the actor who ultimately utilises a given data asset and thus carries the risk of leveraging non-trustworthy data. In the LoA framework, the Data Consumer assesses the provided data trustworthiness assurances to determine whether to use a specific data asset, considering the risks associated with its use.

Data Provider. The Data Provider is the *claimant*. The Data Provider claims that a given data asset provided by them offers a certain degree of trustworthiness. Specifically, by providing a certain Data LoA, the Data Provider claims that appropriate measures were taken to establish a specific degree of confidence in the data asset's trustworthiness.

Assurance Provider. The Assurance Provider should be an independent third-party actor who fulfils the role of a trustworthy auditor and assurer. In the domain of inter-organisational data sharing, it is often referred to as *trust anchor* (CEN/WS TDT, 2024). Although not strictly necessary, having independent audits and assurances greatly enhances the level of trust that a Data Consumer can place in the assured claims – as self-asserted claims are usually not considered trustworthy.

Interactions. To establish a Data LoA, the Data Provider must generate a claim of trustworthiness for a specific data asset. This claim is presented to the Assurance Provider, who conducts an audit of the given claim. To do so, the Data Provider must provide sufficient evidence to prove that their trustworthiness claim indeed holds true. It is then at the discretion of the Assurance Provider to certify the data asset's trustworthiness assurances at a specific level.

Based on the assured claim and its intended application, the Data Consumer can then decide whether to put their confidence in the trustworthiness of the data and utilise it - or not. The final risk and decision responsibility still lies with the Data Consumer, but they now have stronger evidence to inform their decisions and may have legal grounds to sue Data Providers for false assurances.

4.4 Demonstration & Evaluation

We evaluated our initial artifact through demonstration. We followed (Hevner et al., 2004) by opting to conduct an *experimental simulation* as well as an *informed argument* as part of a descriptive evaluation. According to (Gregor and Hevner, 2013), the evaluation through a PoC is sufficient for novel artifacts. We implemented our artifact within data spaces to test our framework for inter-organisational data sharing. This context allowed us to leverage existing technologies for scalable, standardised data sharing and examine the potential impact in practical data sharing scenarios. Our PoC simulates a minimal data space, comprising the following three components, as pictured in Figure 4: *data source*, a *data sink*, and a *data space*.

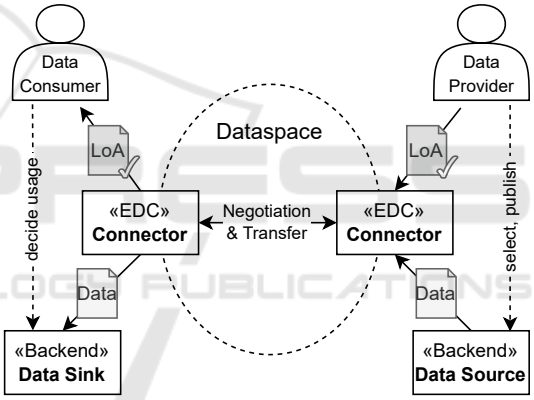

Figure 4: Data LoA PoC experimental setup.

The data space is comprised of two *data space connectors*, which enable a sovereign data exchange between a data provider and consumer. They offer features for data discovery, policy negotiation, and data transfer. The connectors were implemented using the community-driven open-source framework *Eclipse Data Space Components*[3]. The Data Source and Data Sink are simple Python backends aiming to provide or accept dummy data over a REST API. In this PoC, we focus solely on the interaction between the data provider and data consumer to reduce complexity. As a result, all claims are considered self-asserted.

The PoC is deployed using Docker on a virtual machine running Linux Ubuntu. With everything in place, the following steps are performed. First, the provider selects a dataset from their data source to be

[3]https://projects.eclipse.org/projects/technology.edc

published in the data space. The published asset is part of a *data catalog* and describes both the dataset and the usage policies associated with it. In addition, the data provider can include any other information in the data catalog, which, in our case, includes the Data LoA claim generated and associated with the data asset.

Then, the consumer uses their connector to request the provider's catalog and to inspect the registered assets. Typically, a consumer decides whether to request and use a given asset based on the information provided in the catalog. However, this information is oftentimes rather sparse and only contains a general description of the data. When using the Data LoA framework, the data consumer is provided with an additional, comprehensive and standardised Data LoA claim. In this demonstration, we assume the provided claim to be acceptable. Therefore, the consumer decides to request and negotiate the data offer upon which the data is finally transferred.

5 DISCUSSION

In this paper, we present a novel framework for assuring the trustworthiness of data to address the trust deficit of data consumers in inter-organisational data sharing. To establish a comprehensive framework, we followed an objective-oriented DSR approach and identified LoAs as a promising foundation. We then developed a first iteration of our novel Data LoA concept and demonstrated its feasibility through a PoC implementation. We suggest that our work provides the following contributions:

Formalisation of Design Knowledge. To the best of our knowledge, this is the first attempt to explicitly state existing design knowledge and objectives for data trustworthiness artifacts. Using a SLR, we identified three main motivations and one main challenge. We suggest that our work provides a sound foundation for future DSR-based contributions, and we hope that it will lead to the development of new and improved artifacts for data trustworthiness. Our Data LoA is the first contribution to benefit from this formalisation, presenting a novel artifact to address identified challenges in a more comprehensive manner.

Proposal of Data LoA artifact. Based on the identified problem and solution space, we designed an overarching data trustworthiness assurance framework inspired by existing LoAs in the identity domain. Our experimental simulation demonstrated how the Data LoA claim can be presented and exchanged in a typical inter-organisational data sharing environment. We suggest that our solution increases transparency, thereby promoting trust for consumers and enabling them to make sound decisions. This ultimately decreases risk, as consumers are enabled to utilise only data which matches their demands, based on a simple claim.

5.1 Limitations & Future Work

Despite conducting a rigorous design approach, our study is subject to limitations. First, the design knowledge was derived using an SLR approach. We attempted to uncover missing relevant literature by conducting backward and forward searches as part of the SLR. Still, there remains the possibility of unidentified relevant related work.

Second, our artifact is in an early stage. We haven't specified assurance levels yet, as a holistic definition of data trustworthiness must be developed first. We chose to publish this iteration to encourage further work and establish a foundation for future developments. Still, our concept was carefully validated using an experimental simulation.

Third, although interoperability is a design goal, the initial Data LoA concept does not yet address it. It focuses instead on reducing risk, improving trust, and lowering assessment complexity, as noted in prior work. Nonetheless, by adopting the idea of LoA to data trustworthiness, we believe future iterations will tackle this issue.

Given these limitations, we suggest the following future work: First, without a common understanding of data trustworthiness, defining specific LoA levels and ensuring user comprehension remains challenging. Recent standardisation efforts by the CEN working group *Trusted Data Transaction* could provide a promising starting point. (CEN/WS TDT, 2024).

Second, we recommend conducting more DSR cycles to advance the Data LoA framework. In particular, defining specific levels is essential for providers to make accurate claims and for consumers to assess risk properly. We suggest deriving these definitions from ongoing work on risk dimensions and attack taxonomies, as existing LoAs in other domains typically focus on risk. Other aspects of data trustworthiness, such as the reputation of the source or country of origin, should also be considered.

Finally, we suggest identifying relevant domains, drivers for adoption, and potential implementation challenges. This ensures our framework gains wide adoption by clearly communicating target applications, benefits, and trade-offs. For example, (He et al., 2015; Hou et al., 2024) note trade-offs between improving data trustworthiness and factors like cost or privacy. Based on our current understanding, relevant

domains include critical infrastructure or automated systems in sensitive domains such as healthcare or defense. However, AI could also greatly benefit from leveraging data trustworthiness assessments, e.g., to assign different weights to training data based on their Data LoA levels, improving accuracy and reliability.

6 CONCLUSION

This paper presents the novel concept of LoA for data trustworthiness. Data LoA provides a standardised framework to ensure data trustworthiness, addressing the trust deficit of data consumers in inter-organisational data sharing. It aims to enhance trust, reduce risks of using shared data, simplify the assessment of data trustworthiness, and enable interoperability between existing and new approaches. These goals arise from a rigorous DSR approach and the formalisation of existing design knowledge.

We found that although our Data LoA concept addresses most of the identified objectives in theory, more work is needed to deploy it in real scenarios. Especially the goal of interoperability, the level definition and its implementation need more attention. We suggest that further DSR cycles should be performed to incrementally enhance the Data LoA artifact presented here.

Our work contributes to the field of design research for data trustworthiness by formalising design knowledge and presenting a new artifact. We encourage researchers to utilise our findings as a foundation to further investigate the subject. We hope that our contributions help to increase research efforts addressing the identified shortcomings in consumer trust and ultimately improve and extend data sharing activities across organisations.

ACKNOWLEDGEMENTS

CRediT author statement: Florian Zimmer: Conceptualisation, Methodology, Software, Validation, Investigation, Writing - Original Draft, Visualisation. **Janosch Haber:** Conceptualisation, Writing - Review & Editing, **Mayuko Kaneko:** Conceptualisation, Writing - Review & Editing, Project administration.

REFERENCES

Alhaqbani, B. and Fidge, C. (2009). A time-variant medical data trustworthiness assessment model. In *2009 11th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 130–137.

Alkhelaiwi, A. and Grigoras, D. (2015). The origin and trustworthiness of data in smart city applications. In *Proceedings of the 8th International Conference on Utility and Cloud Computing*, UCC '15, pages 376–382. IEEE Press.

Anjomshoaa, A., Elvira, S. C., Wolff, C., Pérez Baún, J. C., Karvounis, M., Mellia, M., Athanasiou, S., Katsifodimos, A., Garatzogianni, A., Trügler, A., Serrano, M., Zappa, A., Glikman, Y., Tuikka, T., and Curry, E. (2022). Data platforms for data spaces. In Curry, E., Scerri, S., and Tuikka, T., editors, *Data Spaces*, Springer eBook Collection, pages 43–64. Springer International Publishing and Imprint Springer, Cham.

Ardagna, C. A., Asal, R., Damiani, E., Ioini, N. E., Elahi, M., and Pahl, C. (2021). From trustworthy data to trustworthy iot: A data collection methodology based on blockchain. *ACM Trans. Cyber-Phys. Syst.*, 5(1).

Bertino, E. (2015). Data trustworthiness—approaches and research challenges. In Garcia-Alfaro, J., Herrera-Joancomartí, J., Lupu, E., Posegga, J., Aldini, A., Martinelli, F., and Suri, N., editors, *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*, volume 8872 of *Lecture Notes in Computer Science*, pages 17–25. Springer International Publishing, Cham.

CEN/WS TDT (July 2024). Trusted data transaction: Part 1: Cwa 18125.

Ebrahimi, M., Tadayon, M. H., Haghighi, M. S., and Jolfaei, A. (2022). A quantitative comparative study of data-oriented trust management schemes in internet of things. *ACM Trans. Manage. Inf. Syst.*, 13(3).

European Parliament (23 July / 2014). Regulation no 910/2014 on electronic identification and trust services fro electronic transactions in the internal market and repealing directive: eidas regulation.

Faheem Zafar, Abid Khan, Saba Suhail, Idrees Ahmed, Khizar Hameed, Hayat Mohammad Khan, Farhana Jabeen, and Adeel Anjum (2017). Trustworthy data: A survey, taxonomy and future trends of secure provenance schemes. *Journal of Network and Computer Applications*, 94:50–68.

Foidl, H. and Felderer, M. (2023). An approach for assessing industrial iot data sources to determine their data trustworthiness. *Internet of Things*, 22:100735.

Gomez, L., Laube, A., and Sorniotti, A. (2009). Trustworthiness assessment of wireless sensor data for business applications. In *2009 International Conference on Advanced Information Networking and Applications*, pages 355–362.

Gregor, S. and Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly*, 37(2):337–355.

Haron, N., Jaafar, J., Aziz, I. A., Hassan, M. H., and Shapiai, M. I. (2017). Data trustworthiness in internet of things: A taxonomy and future directions. In *2017 IEEE Conference on Big Data and Analytics (ICBDA)*, pages 25–30.

He, D., Chan, S., and Guizani, M. (2015). User privacy and data trustworthiness in mobile crowd sensing. *IEEE Wireless Communications*, 22(1):28–34.

Hevner, A. R., March, S. T., Park, J., and Ram, S. (2004). Design science in information systems research. *MIS Quarterly*.

Hou, C., Zhou, C., Wu, C. G., Cong, R., and Li, K. (2024). Optimization of cloud-based multi-agent system for trade-off between trustworthiness of data and cost of data usage. *IEEE Transactions on Automation Science and Engineering*, 21(1):106–122.

Huber, M., Wessel, S., Brost, G., and Menz, N. (2022). Building trust in data spaces. In Otto, B., ten Hompel, M., and Wrobel, S., editors, *Designing Data Spaces*, Springer eBook Collection, pages 147–164. Springer International Publishing and Imprint Springer, Cham.

Islam, M. M., Karmakar, G. C., Kamruzzaman, J., Murshed, M., and Chowdhury, A. (2025). Trustworthiness of iot images leveraging with other modal sensor's data. *IEEE Internet of Things Journal*, 12(1):163–173.

ISO and IEC (April, 2013). Information technology — security techniques — entity authentication assurance framework: Iso/iec 29115.

ISO and IEC (August 2022). Information security, cybersecurity and privacy protection — evaluation criteria for it security - part 5: Iso/iec 15408-5:2022.

Jaigirdar, F. T., Rudolph, C., and Bain, C. (2019). Can i trust the data i see? a physician's concern on medical data in iot health architectures. In *Proceedings of the Australasian Computer Science Week Multiconference*, ACSW '19, New York, NY, USA. Association for Computing Machinery.

Jussen, I., Schweihoff, J., and Möller, F. (2023). Tensions in inter-organizational data sharing: Findings from literature and practice. In *2023 IEEE 25th Conference on Business Informatics (CBI)*, pages 1–10. IEEE.

Karthik, N. and Ananthanarayana, V. S. (2016). Sensor data modeling for data trustworthiness. In *2016 IEEE Trustcom/BigDataSE/ISPA*, pages 909–916.

Leteane, O. and Ayalew, Y. (2024). Improving the trustworthiness of traceability data in food supply chain using blockchain and trust model. *The Journal of The British Blockchain Association*, 7(1):1–12.

Leteane, O., Ayalew, Y., and Motshegwa, T. (2024). A multi-package trust model for improving the trustworthiness of traceability data in blockchain-based beef supply chain. In *IEEE Conference on Dependable and Secure Computing*, pages 155–162.

Lim, H. S., Ghinita, G., Bertino, E., and Kantarcioglu, M. (2012). A game-theoretic approach for high-assurance of data trustworthiness in sensor networks. In *2012 IEEE 28th International Conference on Data Engineering*, pages 1192–1203.

Martínez-Ferrero, J. and García-Sánchez, I.-M. (2018). The level of sustainability assurance: The effects of brand reputation and industry specialisation of assurance providers. *Journal of Business Ethics*, 150(4):971–990.

Nenadic, A., Zhang, N., Yao, L., and Morrow, T. (2007). Levels of authentication assurance: an investigation. In *Third International Symposium on Information Assurance and Security*, pages 155–160. IEEE.

Ormazabal, A., Berry, D., and Hederman, L. (2024). Co-development of a tool to help clinicians decide upon the trustworthiness of patient generated health data. In *2024 IEEE 37th International Symposium on Computer-Based Medical Systems (CBMS)*, pages 442–449.

Otto, B., ten Hompel, M., and Wrobel, S., editors (2022). *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage*. Springer eBook Collection. Springer International Publishing and Imprint Springer, Cham, 1st ed. 2022 edition.

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3):45–77.

Tocco, F. and Lafaye, L. (2022). Data platform solutions. In Otto, B., ten Hompel, M., and Wrobel, S., editors, *Designing Data Spaces*, Springer eBook Collection, pages 383–393. Springer International Publishing and Imprint Springer, Cham.

vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., and Cleven, A. (2015). Standing on the shoulders of giants: Challenges and recommendations of literature search in information systems research. *Communications of the Association for Information Systems*, 37.

von Scherenberg, F., Hellmeier, M., and Otto, B. (2024). Data sovereignty in information systems. *Electronic Markets*, 34(1).

Xu, J. and MacAskill, K. (2023). A carbon data trustworthiness framework for the construction sector. In *Proceedings of the 2023 European Conference on Computing in Construction and the 40th International CIB W78 Conference*. European Council for Computing in Construction.

Zimmer, F., Haber, J., and Kaneko, M. (2025). Enhancing trust in inter-organisational data sharing: Levels of assurance for data trustworthiness - literature body. *Zenodo, https://doi.org/10.5281/zenodo.14639350*.