Towards Levels of Assurance for Data Trustworthiness

A Novel Framework to Promote Trust in Inter-Organisational Data Sharing

Florian Zimmer[1], Janosch Haber[2], Mayuko Kaneko[3] and Takuma Takeuchi[3]

[1] *Fraunhofer Institute for Software and Systems Engineering ISST, Speicherstraße 6, Dortmund, 44147, Germany*
[2] *Fujitsu Research of Europe, 9 Albert St, Slough SL1 2BE, United Kingdom*
[3] *Fujitsu Limited, 4-1-1 Kamikodanaka, Nakahara-ku, Kawasaki, Kanagawa 211-8588, Japan*

Abstract

As data is increasingly acknowledged as a valuable asset, inter-organisational data sharing has recently received much attention. Yet, despite its potential, organisations are still hesitant to engage in data sharing activities, with a lack of trust mentioned as the main barrier. Existing work to mitigate trust barriers usually focuses only on data security concerns or risks from a data provider perspective. In this work, we highlight the unbalanced view on trust and focus on the data usage risks data consumers face. Following design science research, we propose a conceptual, first-iteration artifact called Levels of Assurance for Data Trustworthiness (Data LoA). Data LoA aims to provide an overarching framework to assure data trustworthiness in inter-organisational data sharing. Assuring data trustworthiness is suggested to improve data consumers' risk assessment and decision-making capabilities, and enhances trust and transparency between data providers and consumers. This paper is focused on outlining central mechanisms of our new concept, intending to facilitate a wider discussion on the technical and social aspects and requirements of establishing data trustworthiness.

Keywords

Data Trustworthiness, Levels of Assurance, Inter-Organisational Data Sharing, Trust, Data Spaces

1. Introduction

In an increasingly interconnected world, data is acknowledged as one of the key drivers of innovation and growth in business and society [1]. Consequently, inter-organisational data sharing has recently gained much attention from both researchers and practitioners, aiming to unlock the full potential of data by sharing it across organisational and country borders [2].

Despite its potential, in practise, organisations often hesitate to engage in data sharing activities. Research suggests that a lack of trust and transparency are among the most fundamental barriers hindering a widespread adoption of inter-organisational data sharing [3]. Addressing these factors, significant effort has been put into the development of *data spaces* that address central *data sovereignty* concerns of *data providers* by enabling them to maintain control over their data [1].

A main concern of *data consumers*, on the other hand, is the risk of utilising third-party data, e.g. for (automated) decision-making, without reliable means to assess its quality, integrity and trustworthiness. [4, 1, 2]. However, as data usage risks can range from financial losses to human harm [5, 6] data consumers usually have no other option than to put their trust in the data provider, as trust cannot be established on the data level itself [7].

In this study, we argue that equipping data consumers with improved risk assessment and decision-making capabilities contributes to completing the previously imbalanced perspective on data sharing risks, and that establishing the trustworthiness of shared data assets themselves could be a key enabling factor to accelerate the adoption of inter-organisational data sharing. Following a *design*

[*] *RCIS 2025 Workshops and Research Projects Track. 20 - 23 May, 2025. Seville, Spain.*

[1*] Corresponding author.

florian.zimmer@isst.fraunhofer.de (F. Zimmer); janosch.haber@fujitsu.com (J. Haber); k.mayuko@fujitsu.com (M. Kaneko); takeuchi.takuma@fujitsu.com (T. Takeuchi)

0009-0002-8060-7162 (F. Zimmer); 0000-0001-5494-9770 (J. Haber); 0000-0001-9873-2557 (M. Kaneko); 0009-0002-7782-5839 (T. Takeuchi)

science research (DSR) approach, we develop a new artifact to bridge the gap between existing approaches to assure data trustworthiness and the complex requirements of inter-organisational data sharing. As a result, we propose *Levels of Assurance for Data Trustworthiness* (Data LoA), a novel framework aimed at enhancing trust and transparency among data providers and consumers. Being a first-iteration artifact, this work focuses on fundamental ideation, outlining key actors, their interactions, and potential data trustworthiness dimensions. We demonstrate the technical application of a first subset of Data LoA features by implementing a *proof of concept* (PoC) and conducting an experimental simulation based on a real use case scenario in the *Mobility Data Space*. Trust, however, is a complex socio-technical and context-dependent, subjective assessment that goes beyond pure technical measures. The purpose of this paper, therefore, is to articulate our novel concept and facilitate a wider discussion on the different aspects and requirements of functional data trustworthiness.

2. Related Work

Data trustworthiness has been studied extensively across various domains and applications such as healthcare, defence, traffic control, and manufacturing [8]. Previous work has produced a wide range of different solutions to measure, assess, and assure data trustworthiness, especially in the contexts of *internet of things* (IoT) and *mobile crowd sensing* (MCS). Many solutions accomplish this by binding data trustworthiness to different metrics and dimensions.

In [9], for instance, the authors propose a trust score model to measure the trustworthiness of industrial IoT data sources based on accuracy definitions established by an expert panel. Conversely, in [10], the authors aim to increase data trustworthiness in IoT by estimating it based on syntactic and semantic rules, considering data origin and time of creation. Similar approaches determine data trustworthiness based on the similarity of multiple sensor readings in close proximity [11]. In [12], the authors opt for a more holistic approach, proposing a data trustworthiness framework for carbon data in the construction sector. Mentioning data availability, quality, security, and compatibility, the authors aim to provide clear actions to increase the trustworthiness of data as it is generated and managed.

Most solutions establish data trustworthiness through transparency, either by communicating relevant aspects directly or by assembling and providing some kind of trust score. However, as most of these solutions are tailored to a specific use case, they recognise different ways of assessing data trustworthiness. Thus, none of them is designed with interoperability in mind, failing to provide a comprehensive view of data trustworthiness, especially in the context of inter-organisational data sharing. We, therefore, argue that a more general, overarching solution is needed that clearly articulates relevant dimensions of data trustworthiness and defines transparent processes on how to assure and assess it across organisational and legislative borders.

A promising solution to overcome this fragmented landscape is *levels of assurance* (LoA). LoA is an assurance technique to improve and simplify risk management and decision-making capabilities to evaluate and grade complex scenarios [13]. The concept of LoA has been predominantly used in the domain of identity validation, e.g. in the ISO/IEC 29115[2] standard for authentication assurance or in the eIDAS[3] directive declared by the EU to address the fragmented landscape of verification schemes across member states. Another well-known identity LoA is the NIST-800-63-A[4] guideline. They all specify a range of concrete levels (such as high, substantial, and low), clearly defining what processes, management activities, and technologies must be employed to reach a certain degree of confidence in the assured claim. That means the more measurements are in place to ensure a given claim, the higher the LoA. However, although there are many different LoAs already, none exist for assuring and assessing the trustworthiness of data. To the best of our knowledge, we are the first to adapt LoA to data trustworthiness to meet the requirements of complex inter-organisational data sharing scenarios.

[2] https://iso.org/standard/45138.html [11.03.25]

[3] https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation [11.03.25]

[4] https://pages.nist.gov/800-63-3/sp800-63a.html [11.03.25]

3. Methodology

In this paper, our goal is to address the lack of trust from the perspective of data consumers. We conducted a rigorous DSR approach following Peffers et al. [14] to design a novel Data LoA artifact, providing a framework for unifying and standardising the assurance of data trustworthiness in inter-organisational data sharing. More specifically, we followed an *objective-centred* DSR approach, building upon existing data trustworthiness assuring and measuring artifacts. However, as previous solutions were not necessarily developed using DSR, available design knowledge was limited. Therefore, we began by mapping the problem and solution space, identifying challenges, solutions, and goals by conducting a *structured literature review* (SLR) following vom Brocke et al. [15].

We started with an exploratory pre-study using Google Scholar to increase familiarity with the subject. Next, we conducted a keyword-based search and screenlining process to select relevant articles, and performed back- and forward searches as recommended in [15] to achieve improved coverage. Ultimately, this led to the identification of a total of 62 articles, which we labelled by domain and artifact type based on the taxonomy proposed in [16], i.e. conceptual, mathematical, architectural and framework. Additionally, we identified frequently mentioned motivations, challenges, and common objectives for individual solutions. This analysis was done to ensure the relevancy of our artifact and to inform our design efforts. Lastly, we collected all occurrences of aspects mentioned in literature related to data trustworthiness to provide a broad perspective on different notions of trust. The conducted research process is outlined in Figure 1. The complete labelled literature body is made accessible for full transparency in [17].

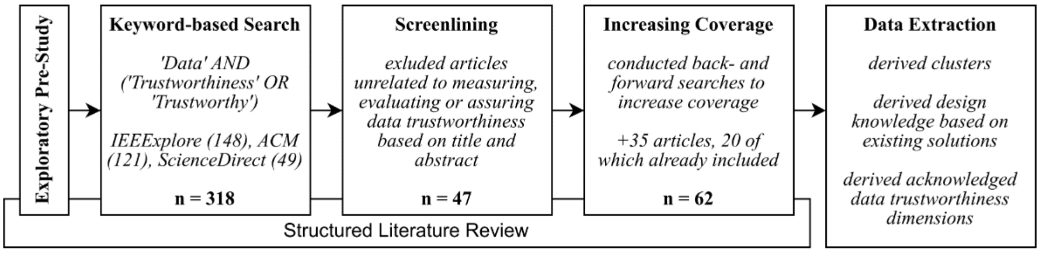
Exploratory Pre-Study
Keyword-based Search
'Data' AND ('Trustworthiness' OR 'Trustworthy')
IEEExplore (148), ACM (121), ScienceDirect (49)
n = 318
Screenlining
exluded articles unrelated to measuring, evaluating or assuring data trustworthiness based on title and abstract
n = 47
Increasing Coverage
conducted back- and forward searches to increase coverage
+35 articles, 20 of which already included
n = 62
Data Extraction
derived clusters
derived design knowledge based on existing solutions
derived acknowledged data trustworthiness dimensions
Structured Literature Review

Figure 1: Methodology to derive foundation of knowledge to inform our research and DSR work.

We then followed DSR methodology in defining a set of design objectives based on our SLR and developed a novel, first-iteration artifact. Our design process aimed to address the shortcomings of existing work by grounding our development efforts on the existing LoA concept, as this seemed to be a promising solution aligned with the identified design goals. Being a first-iteration artifact, we focused on defining key mechanisms, actors and their relations to establish a sound foundation for future iterations. In the third and fourth steps of DSR, we evaluated our concept through instantiating a PoC using data spaces, providing a field-tested environment for inter-organisational data sharing. This experimental simulation allowed us to investigate the technical feasibility of our concept and determine limitations and considerations for future work.

4. Proposed Solution

4.1. Motivations and Objectives

As we intend our novel framework to address the shortcomings of previous work, we first had to map out and analyse the problem space. To do so, in [18], we present the results of an extensive SLR, deriving frequently mentioned motivations and common objectives to inform our design efforts.

We found that research agrees on the accuracy and reliability of services, operations, and decision-making being closely coupled to the data they are based on [19, 20]. As a result, utilising untrustworthy, low-quality data can lead to severe consequences, as past incidents in healthcare and power supply demonstrated [5, 6]. Additionally, increasingly automated operations are demanding a growing amount of data [21, 11]. As a result, most solutions aim to increase transparency by measuring or assuring data trustworthiness to allow for better risk assessment capabilities. This is usually done by providing an in-depth view of the data's provenance [22], or by providing an easier-to-comprehend trust score [9]. However, while increasing data trustworthiness can greatly enhance the accuracy and reliability of operations conducted with this data, it is also suggested that assuring and increasing data trustworthiness can be challenging due to the number of aspects involved in establishing it [21].

Besides adopting commonly agreed-on key motivations and goals to guide our design efforts, we also consider an additional design objective: we found that although most solutions share a common view of the issue and a shared set of goals, they were not designed with interoperability in mind. Yet, given the challenging task of ensuring data trustworthiness, we are confident that a holistic solution is needed — one in which existing solutions might be part of solving the bigger picture. Therefore, we consider the design objective of interoperability in our design efforts, aiming to develop an overarching solution to meet the requirements of the complex environment of inter-organisational data sharing.

4.2. Framework for Establishing Levels of Assurance for Data Trustworthiness

To enhance trust in inter-organisational data sharing and increase risk assessment and decision-making capabilities for consumers, we propose Data LoA, a novel assurance framework to promote trust through increased transparency. Following DSR, our proposed concept is a first-iteration artifact, focusing on central actors and their relations. Similar to existing LoAs within other domains, Data LoA is defined as *the degree of confidence that a data asset's underlying information can be trusted to be true.* In other words, Data LoA seeks to assure the level of confidence that a data consumer can put into the trustworthiness of a given data asset, considering the remaining risks they face with respect to trust attributes not included in the provided assurance.

To establish the Data LoA framework, we propose to define a range of components to capture different aspects of ensuring, measuring, claiming, assuring, and assessing the trustworthiness of data assets. Specifically, we propose that our data trustworthiness framework should contain:

1. a clearly defined **actor model** that stipulates the different roles, responsibilities and liabilities of the parties involved in inter-organisational data sharing
2. an application-driven definition of relevant **trustworthiness dimensions** to be considered for assuring and assessing data trustworthiness
3. a suitable **data usage risk model** that can be used to identify and assess the risks connected to utilising third-party data in a given data-driven application
4. a clear definition of a few concrete **trustworthiness assurance levels** enabling data providers to make trustworthiness claims and data consumers to evaluate them
5. a clear, practical **guide for selecting** appropriate **trustworthiness levels** for data consumers given their determined data usage risks
6. a broadly accepted **audit model** for certifying, as well as auditing and assuring trust ensuring measures, including the selection and certification of appropriate assurance providers

In the following, we provide initial considerations for the first two of these subcomponents.

4.3. Data LoA Actor Model

Within Data LoA we define three main actors: Data Consumer, Data Provider and Assurance Provider. All actors, as well as their relations, are displayed in Figure 2.

Data provider and consumer are the main parties commonly encountered in typical data sharing use cases, with one party providing the data asset and the other consuming it. In the context of LoA, data providers are called *claimants*, as they claim the degree of trustworthiness of their asset. Data consumers are referred to as *risk owners*, as they face the risks of relying on third-party data assets.

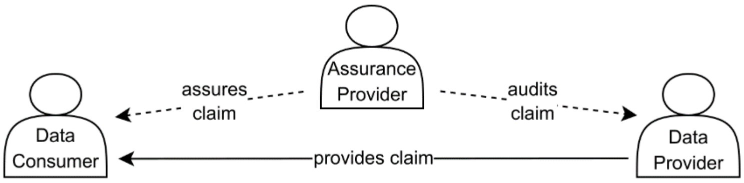

Figure 2: Actor model of Data LoA, based on Zimmer et al. [18].

For a data consumer to decide what level of trustworthiness their application requires, their data usage-related risks must be assessed. Knowing these risks, consumers can consider provided data trustworthiness claims and decide whether these sufficiently address their risks. However, as self-assured claims are usually not considered trustworthy, we suggest that a third-party assurance provider should be introduced to assure given claims - either by certifying the means of creating and ensuring a data asset or by auditing the created asset. Depending on the scenario, multiple assurance providers might be required to audit individual trust attributes.

Being a first-iteration artifact, it needs to be highlighted that it is not yet clear how the different levels should be defined, how to assess data usage risks, or how to establish and communicate trustworthiness claims. Taking a first step towards addressing these central issues, we provide a preliminary overview of what dimensions of data trustworthiness are likely needed to be considered.

4.4. Data Trustworthiness Dimensions

Much research has been conducted on the topic of data trustworthiness across a variety of domains and applications. However, a high degree of context and domain dependency so far have prevented the formulation of a generally accepted notion of data trustworthiness [21, 12]. Still, most research agrees on data trustworthiness being described as *the possibility to ascertain the correctness of data provided by a data source* [19]. Taking a first step towards a uniform definition, we conducted a SLR to identify relevant dimensions in the previously identified existing literature on data trustworthiness. The results are displayed in Table 1.

Table 1
Mentioned dimensions of data trustworthiness, descending based on occurrences.

	#		#		#		#		#
Origin	20	Correctness	11	Quality	8	Availability	2	Confidentiality	1
Integrity	19	Similarity	11	Authenticity	8	Veracity	2	Validity	1
Provenance	14	Accuracy	10	Timeliness	5	Compatibility	1		
Security	11	Reliability	9	Completeness	4	Credibility	1		

In total, we found 18 different dimensions mentioned in literature. A full overview of the annotated literature body can be found in [17]. The most mentioned dimensions of data trustworthiness are *data origin*, *integrity*, and *provenance*. This indicates that the trustworthiness of the source, as well as maintaining data integrity and being able to backtrack the actors and manipulations involved in the data lifecycle, are recognised as significant factors in determining the data's trustworthiness. Besides that, *data security*, *correctness*, *similarity*, and *accuracy* are also considered substantial factors. While security, correctness and accuracy are hard to argue, data similarity is often mentioned in IoT, determining data's trustworthiness by comparing data of multiple sensors sensing the same event [11].

It is worth noting that some dimensions overlap to varying degrees. Data security, for example, is usually also concerned with maintaining data integrity, while data origin can be considered to be an element of data provenance. Finally, *data quality* seems closely related to data trustworthiness, with some previous publications using these terms interchangeably [12]. Following the ISO/IEC 25012:2008[5] data quality model, data quality is, among others, comprised of accuracy, completeness, credibility, currentness, availability, and confidentiality - emphasising the extensive overlap. Consequently, our findings confirm the lack of a commonly agreed-on notion of data trustworthiness, which will be a central pre-requisite for defining concise levels of data trustworthiness required by our framework.

4.5. Demonstration

To demonstrate the Data LoA framework, we illustrate its real-world application in the *Mobility Data Space*, a data sharing ecosystem for real-time traffic data and sensitive mobility data [23]. A key application for this data is to provide real-time information about traffic conditions and travel times for daily commutes. However, as data providers comprise a constantly changing, diverse set of public transport operators, road authorities, traffic management systems, private fleets and mobile network operators, ensuring pre-existing trust relations is virtually impossible. As a result, data consumers often have no means of assessing the trustworthiness of available data.

This use case highlights a number of value drivers for the Data LoA concept: i) the data itself is valuable. It needs to be brought together to allow for impactful real-time predictions, which means that data consumers are incentivised to compensate data providers, who in turn are motivated to provide their data for a secondary value chain; ii) the data is big, complex, and decentralised and requires extensive data sharing to unlock its full value; iii) there is a large amount of data providers that cannot all be explicitly trusted; iv) the data usage risks are concrete, as incorrect predictions will lead to damages to reputation and loss of business for the data consumer.

Based on the described scenario, we conducted an experimental evaluation by implementing a PoC to demonstrate the practical implications Data LoA has. To reduce complexity, we simplified the use case down to a minimal data space, i.e., one connector for each party and a data sink and data source, respectively. The PoC's scope and setup are displayed in Figure 3.

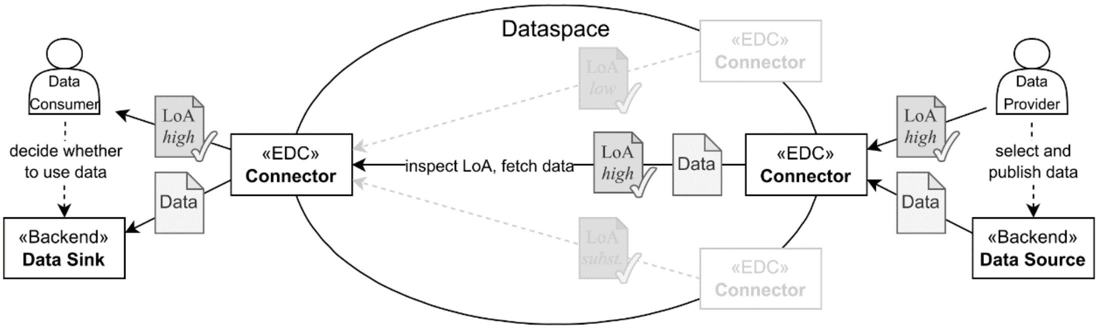

Figure 3: An overview of the PoC implementation, based on Zimmer et al. [18].

To realise the data space, we utilised the *Eclipse Dataspace Components*[6] framework, as this allowed for a sophisticated data-sharing environment. Data source and sink were implemented using Python, offering simple data-providing and -consuming REST APIs. The PoC was deployed using Docker on a virtual machine running Linux Ubuntu 24.04.2 LTS.

In the experiment, the provider first selects and publishes a data asset from their data source, including the Data LoA certificate in the data asset's custom fields. We used X.509 certificates to include the assured claim in the certificate's extension field. This links the assured claim directly to the data asset, and both are made available in the data space using the *data catalog* - an overview of available data assets. Based on this, the consumer is able to make an informed decision about utilising the data or not, using the appended Data LoA certificate with its assured claim. Using X.509 certificates provides

[5] https://www.iso.org/standard/35736.html [11.03.25]

[6] https://projects.eclipse.org/projects/technology.edc [11.03.25]

an easy way to get the assured claim validated by the certificate issuer, namely the assurance provider. We omitted the assurance provider from the demonstrator at this stage for clarity. Nevertheless, we validated how the provider can effectively communicate the Data LoA claim, and it is made available to the consumer in inter-organisational data sharing in the sophisticated environment of data spaces.

5. Discussion

In this paper we present a novel, conceptual framework for assuring the trustworthiness of third-party data assets to address data consumer trust barriers in inter-organisational data sharing. Based on our findings, we are confident that the Data LoA concept will mitigate data usage risks for data consumers, enabling them to make informed decisions when selecting what data to utilise and avoid relying on untrustworthy data in high-risk environments. With the Data LoA framework, data consumers do not have to rely solely on trust on an organisational level. Instead, they are able to assess trust at a data level, enhancing overall trust in inter-organisational data sharing by increasing transparency. However, being a first-iteration artifact, there remain a number of open questions and issues to address.

5.1. Limitations and Future Work

Despite following a rigorous research approach, our work is subject to limitations. First, we grounded our DSR approach on derived design knowledge using a SLR. Naturally, literature reviews are limited by their coverage. Therefore, we attempted to mitigate this by conducting for- and backward searches. Still, there remains the possibility of unidentified related work.

Second, Data LoA is at an early stage. As a first-iteration artifact, central open questions remain, including how to define meaningful, concrete trustworthiness levels, how to assess data usage risks in a generalisable fashion, and how to establish, communicate and assess trustworthiness claims. Additionally, the goal of interoperability was not addressed by the PoC demonstrator presented, and establishing trustworthiness has predominantly been approached from a technical perspective, leaving many open issues around legal and social responsibility as well as liability.

We suggest the following future work: First, more work is urgently needed to create a sound working definition of data trustworthiness and its dimensions. This work provided a first overview of potential data trustworthiness dimensions, however, further research is needed to develop a more concise notion, enabling all participants to understand and issue data trustworthiness-related claims. A promising consortium for this matter might be the CEN working group of *Trusted Data Transaction*, as it aims to identify trust characteristics of data transactions [24].

Second, more work is required on the application of Data LoA: Data providers need to understand how to establish a claim, while assurance providers need to know how to audit such claims, whereas data consumers need to be enabled to select an appropriate level. As LoAs are defined risk-based, data usage risks need to be identified and a selection process established for consumers to make sound decisions. A promising starting point is existing LoAs like NIST-800-63-A, providing a decision tree to guide level selection for identity LoA. Thus, future DSR cycles should address these issues.

Finally, Data LoA needs to be contextualised: Relevant domains, applications, drivers, and incentives must be identified. This ensures widespread adoption of the framework, clearly communicating its benefits and trade-offs one must consider when opting to employ it. For instance, in [25] the authors mention cost and privacy factors involved in ensuring data trustworthiness. Based on our current understanding, relevant domains could, e.g., be in critical infrastructure, automated systems in highly sensitive domains, or artificial intelligence in data-scarce environments, as it allows to weigh training data based on their LoA, potentially achieving higher accuracy.

6. Conclusion

In this paper, we present the novel concept of Data LoA, a first-iteration DSR artifact. Data LoA aims to provide a comprehensive, standardised framework to assure the trustworthiness of data, addressing data consumers' trust barriers in inter-organisational data sharing. Data LoA is proposed to improve data consumers' risk assessment and decision-making capabilities by enhancing transparency and mitigating the risks they face when relying on third-party data assets. Having demonstrated a PoC implementation in the context of data spaces, we are confident that the Data LoA framework is capable of enhancing trust in inter-organisational data sharing, driving its adoption.

We found that although Data LoA addresses most of the identified challenges and objectives in theory, more work is needed until our framework is ready for adoption. Especially a sound working definition of data trustworthiness and a concrete definition of assurance levels are needed to realise the Data LoA concept. We suggest that further DSR cycles should be performed to tackle the remaining open issues incrementally and hope that this paper facilitates a wider discussion on the technical and social aspects and requirements of establishing data trustworthiness.

Acknowledgements

The authors would like to thank their team members at Fraunhofer ISST and Fujitsu Research of Japan for insightful discussions and the reviewers of the BPMS2 2025 workshop for their prompt and constructive feedback.

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

Declaration on Generative AI

During the preparation of this work, the author(s) used Grammarly in order to: Grammar and spelling check & Improve writing style. After using these tool(s)/service(s), the author(s) reviewed and edited the content as needed and take(s) full responsibility for the publication's content.

References

[1] B. Otto, M. ten Hompel, S. Wrobel (Eds.), Designing Data Spaces: The Ecosystem Approach to Competitive Advantage, Springer eBook Collection, 1st ed. 2022 ed., Springer International Publishing and Imprint Springer, Cham, 2022. doi:10.1007/978-3-030-93975-5.

[2] F. Tocco, L. Lafaye, Data Platform Solutions, in: B. Otto, M. ten Hompel, S. Wrobel (Eds.), Designing Data Spaces, Springer eBook Collection, Springer International Publishing and Imprint Springer, Cham, 2022, pp. 383–393. doi:10.1007/978-3-030-93975-5_23.

[3] I. Jussen, J. Schweihoff, F. Möller, Tensions in Inter-Organizational Data Sharing: Findings from Literature and Practice, in: 2023 IEEE 25th Conference on Business Informatics (CBI), IEEE, 2023, pp. 1–10. doi:10.1109/CBI58679.2023.10187530.

[4] Faheem Zafar, Abid Khan, Saba Suhail, Idrees Ahmed, Khizar Hameed, Hayat Mohammad Khan, Farhana Jabeen, Adeel Anjum, Trustworthy data: A survey, taxonomy and future trends of secure provenance schemes, Journal of Network and Computer Applications 94 (2017) 50–68. doi:10.1016/j.jnca.2017.06.003.

[5] H. S. Lim, G. Ghinita, E. Bertino, M. Kantarcioglu, A Game-Theoretic Approach for High-Assurance of Data Trustworthiness in Sensor Networks, in: 2012 IEEE 28th International Conference on Data Engineering, 2012, pp. 1192–1203. doi:10.1109/ICDE.2012.78.

[6] F. T. Jaigirdar, C. Rudolph, C. Bain,Can I Trust the Data I See? A Physician's Concern on Medical Data in IoT Health Architectures, in: Proceedings of the ACSW Multiconference, ACSW'19, Association for Computing Machinery, New York, NY, USA, 2019. doi:10.1145/3290688.3290731.

[7] B. Alhaqbani, C. Fidge, A Time-Variant Medical Data Trustworthiness assessment model, in: 2009 11th International Conference on e-Health Networking, Applications and Services (Healthcom), 2009, pp. 130–137. doi:10.1109/HEALTH.2009.5406198.

[8] L. Gomez, A. Laube, A. Sorniotti, Trustworthiness Assessment of Wireless Sensor Data for Business Applications, in: 2009 Int. Conf. on AINA, 2009, pp. 355–362. doi:10.1109/AINA.2009.92.

[9] H. Foidl, M. Felderer, An approach for assessing industrial IoT data sources to determine their data trustworthiness, Internet of Things 22 (2023) 100735. doi:10.1016/j.iot.2023.100735.

[10] C. A. Ardagna, R. Asal, E. Damiani, N. E. Ioini, M. Elahi, C. Pahl, From Trustworthy Data to Trustworthy IoT: A Data Collection Methodology Based on Blockchain, ACM Trans. Cyber-Phys. Syst. 5 (2021). doi:10.1145/3418686.

[11] M. M. Islam, G. C. Karmakar, J. Kamruzzaman, M. Murshed, A. Chowdhury, Trustworthiness of IoT Images Leveraging With Other Modal Sensor's Data, IEEE Internet of Things Journal 12 (2025) 163–173. doi:10.1109/JIOT.2024.3459477.

[12] J. Xu, K. MacAskill, 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, 2023. doi:10.35490/ec3.2023.261.

[13] A. Nenadic, N. Zhang, L. Yao, T. Morrow, Levels of Authentication Assurance: an Investigation, in: 3rd Int. Symp. on Inf. Assurance and Security, IEEE, 2007, pp. 155–160. doi:10.1109/IAS.2007.88.

[14] K. Peffers, T. Tuunanen, M. A. Rothenberger, S. Chatterjee, A Design Science Research Methodology for Information Systems Research, Journal of Management Information Systems 24 (2007) 45–77. doi:10.2753/MIS0742-1222240302.

[15] J. vom Brocke, A. Simons, K. Riemer, B. Niehaves, R. Plattfaut, A. Cleven, Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research, CAIS 37 (2015). doi:10.17705/1CAIS.03709.

[16] F. M. R. Junior, C. A. Kamienski, A Survey on Trustworthiness for the Internet of Things, IEEE Access 9 (2021) 42493–42514. doi:10.1109/ACCESS.2021.3066457.

[17] F. Zimmer, J. Haber, M. Kaneko, T. Takeuchi, Towards levels of assurance for data trustworthiness - literature body, 2025. doi:10.5281/zenodo.15034965.

[18] F. Zimmer, J. Haber, M. Kaneko, Enhancing Trust in Inter-Organisational Data Sharing: Levels of Assurance for Data Trustworthiness, in: Proceedings of the 14th International Conference on Data Science, Technology and Applications - DATA, INSTICC, SciTePress, 2025, to appear.

[19] N. Haron, J. Jaafar, I. A. Aziz, M. H. Hassan, M. I. Shapiai, Data trustworthiness in Internet of Things: A taxonomy and future directions, in: 2017 IEEE Conference on Big Data and Analytics (ICBDA), 2017, pp. 25–30. doi:10.1109/ICBDAA.2017.8284102.

[20] N. Karthik, V. S. Ananthanarayana, Sensor Data Modeling for Data Trustworthiness, in: 2016 IEEE Trustcom/BigDataSE/ISPA, 2016, pp. 909–916. doi:10.1109/Trustcom/BigDataSE/ICESS.2017.330.

[21] E. Bertino, Data Trustworthiness—Approaches and Research Challenges, in: J. Garcia-Alfaro, J. Herrera-Joancomartí, E. Lupu, J. Posegga, A. Aldini, F. Martinelli, N. Suri (Eds.), Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance, volume 8872 of *Lecture Notes in Computer Science*, Springer International Publishing, Cham, 2015, pp. 17–25. doi:10.1007/978-3-319-17016-9_2.

[22] O. Leteane, Y. Ayalew, T. Motshegwa, A Multi-Package Trust Model for Improving the Trustworthiness of Traceability Data in Blockchain-Based Beef Supply Chain, in: 2024 IEEE Conference DSC, 2024, pp. 155–162. doi:10.1109/DSC63325.2024.00040.

[23] S. Pretzsch, H. Drees, L. Rittershaus, C. Schlueter-Langdon, C. Weiers, Mobility Data Space Whitepaper, 2021. URL: https://www.mobility-data-space.de/content/dam/ivi/mobility-data-space/ documents/Mobility_Data_Space_DE_20220603_web.pdf.

[24] European Committee for Standardization, Trusted Data Transaction: Part 1, July 2024. URL: https://www.trusted-data-transaction.org/en/.

[25] C. Hou, C. Zhou, C. G. Wu, R. Cong, K. Li, 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 (2024) 106–122. doi:10.1109/TASE.2022.3224984.