Systematizing Different Types of Interfaces to Interact with Data Trusts

Research Paper

David Acev[1], Florian Rieder[1], Dennis M. Riehle[1], and Maria A. Wimmer[1]

[1] University of Koblenz, Institute for IS Research, Koblenz, Germany
{dacev, rieder, riehle, wimmer}@uni-koblenz.de

Abstract. The interactions between Data Trusts as fiduciary data sharing intermediaries and data actors communicating with Data Trusts need to be seamless and supported by guidelines and regulatory standards to ensure trustworthiness. To achieve such coherent data sharing, corresponding interfaces have to be designed on human-system as well as on system-system level. In a data trust ecosystem, human interaction of the data actors with the Data Trust is accomplished via user interfaces, i.e. the human-system interaction in the ecosystem. The interaction on the system-system level is manifested through technical interfaces established in Data Trusts. To ensure standardized data sharing, Data Trusts need to be competent in handling different data structures and to provide suitable connections with data storages. We conduct a systematic analysis of existing human and technical interfaces in literature, and we highlight gaps and insufficiently considered topics that are valuable for the implementation of Data Trusts.

Keywords: Data Trust, user interface, API, interoperability, data sharing

1 Introduction

The increase of data volumes together with the rising demand for data to deliver intelligent services has emphasized the need for sharing and reusing data on the one hand, and for managing data through indestructible, trustworthy data governance mechanisms on the other hand. For the latter, scholarly literature refers to data governance as the structures, people, policies, processes, standards, and technologies that govern the management and use of data within an organization to circumvent any potential obstacles in the data sharing process that could result in lack of trust between entities (Abraham et al., 2019; Panian, 2010; Steinert & Altendeitering, 2024). For the data sharing and reuse, the concept of Data Trust has evolved as an important intermediary.

O'Hara (2019) refers to Data Trust as an intermediary organization that implements data sharing. It works in line with the laws and norms to provide ethical, architectural and governance support for secure and trustworthy data processing (O'Hara, 2019). Data Trusts enhance data accessibility, transparency, security, and compliance with relevant regulations and ethical standards throughout the data lifecycle in the ecosystem

20th International Conference on Wirtschaftsinformatik,
September 2025, Münster, Germany

(Austin & Lie, 2021; Ayappane et al., 2024; Feth & Rauch, 2024; Stachon et al., 2023). While many scholars focus on data governance practices to foster collaboration and data sharing processes within the organization, it is also crucial to expand the concept on an inter-organizational basis. Thus, inter-organizational data governance related to Data Trusts involves contractual agreements, data usage policies, distributed usage control, metadata management, licenses, reference processes, and measures for data integration (Abraham et al., 2019; Lis et al., 2023; Otto & Jarke, 2019).

To guarantee well-regulated data workflows between different actors (stakeholders), Data Trusts act like an interface between these stakeholders (O'Hara, 2019). However, this concept of "interface" needs to be detailed on two strands: human-system interaction and system-system interaction. The interfaces need to be interconnected with each other to accomplish smooth data sharing between different entities by enhancing data interoperability (Gruson-Daniel et al., 2023). According to the European Interoperability Framework (EIF), interoperability is "*the ability of organizations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organizations, through the business processes they support, by means of the exchange of data between their ICT systems*" (European Commission, 2017). The definition provided in the EIF considers interoperability holistically at the legal, organizational, semantic, and technical levels. Semantic interoperability in particular ensures that the precise format and meaning of exchanged data and information are preserved and understood throughout data exchanges between parties (European Commission, 2017, p. 25). It enables computer systems and applications to unambiguously interpret, and process data transmitted to them (Mohamed et al., 2012).

To achieve afore mentioned aims, interfaces represent a crucial part of the implementation of Data Trusts, as these enable a smooth exchange of data between data actors. Yet, a comprehensive understanding and systematization of different types of interfaces in the realm of Data Trusts is still lacking.

Our research therefore focuses on the concept of Data Trusts (in some literature referred to as Data Trustees) and the designed and integrated interfaces to enable seamless data sharing and interaction of data actors with the Data Trust. To gain an extensive understanding of existing work and to extract valuable insights and gaps in the current developments in interface implementations in Data Trusts, our study systematically analyzes existing literature on Data Trusts and their implemented interfaces. Two major research objectives (ROs) drive our work:

RO1: Investigating current research on interfaces for implementing Data Trusts;
RO2: Identifying existing mechanisms for accessing different data structures and databases in the realm of Data Trusts.

To meet these ROs, we apply a systematic, topic-centric literature analysis as described in Section 2. In Section 3, we address RO1 by providing a literature review of currently implemented or proposed interfaces in the construction of Data Trusts or in other organizations that could be used in Data Trusts. Section 4 addresses RO2 by presenting existing implementations and suggestions for coping with different data structures, and for interfaces to the data storages. In Section 5 and 6, we pinpoint the main findings of our study and outline future research needs and limitations of our study.

2 Methodological Foundations

We apply a systematic study of peer-reviewed scientific literature, following the guidelines of structured, topic-centric literature review (Rowe, 2014; vom Brocke et al., 2015; Webster & Watson, 2002). Figure 1 visualizes the search process of our systematic research following the PRISMA 2020 flow diagram proposed in Page et al. (2021).

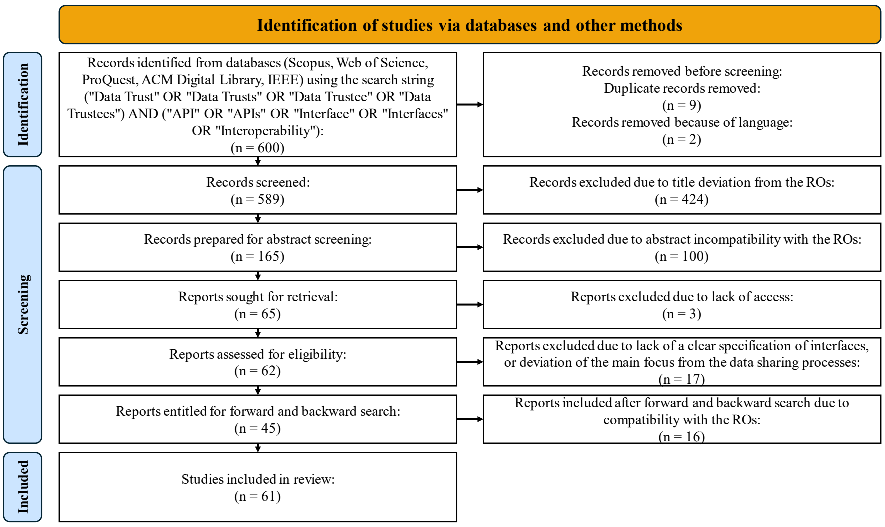
Identification of studies via databases and other methods
Identification
Records identified from databases (Scopus, Web of Science, ProQuest, ACM Digital Library, IEEE) using the search string ("Data Trust" OR "Data Trusts" OR "Data Trustee" OR "Data Trustees") AND ("API" OR "APIs" OR "Interface" OR "Interfaces" OR "Interoperability"): (n = 600)
Records removed before screening: Duplicate records removed: (n = 9) Records removed because of language: (n = 2)
Screening
Records screened: (n = 589)
Records excluded due to title deviation from the ROs: (n = 424)
Records prepared for abstract screening: (n = 165)
Records excluded due to abstract incompatibility with the ROs: (n = 100)
Reports sought for retrieval: (n = 65)
Reports excluded due to lack of access: (n = 3)
Reports assessed for eligibility: (n = 62)
Reports excluded due to lack of a clear specification of interfaces, or deviation of the main focus from the data sharing processes: (n = 17)
Reports entitled for forward and backward search: (n = 45)
Reports included after forward and backward search due to compatibility with the ROs: (n = 16)
Included
Studies included in review: (n = 61)

Figure 1. Systematic Literature Analysis along the PRISMA Statement of Page et al. (2021)

The search was conducted on the databases: Scopus, Web of Science, ProQuest, ACM Digital Library, and IEEE. We used the search string ("Data Trust" OR "Data Trusts" OR "Data Trustee" OR "Data Trustees") AND ("API" OR "APIs" OR "Interface" OR "Interfaces" OR "Interoperability"). This keyword-based search string successfully discarded the possibility of undesirable bias towards renown authors and highly cited papers. The performed search was focused on English language sources. The time period of searched papers was restricted from January 2010 to February 2025. This restriction was applied because before the year 2010, there were barely any robust publications on Data Trusts. The initial search, which was done in February 2025, yielded 600 papers. Eliminating duplicates and papers not in English language reduced the number to 589 papers, concluding the first and second iterations of the analysis. The third iteration screened the titles to identify the papers relevant to our ROs (RO1 and RO2), which resulted in 165 papers, hence excluding 424 papers not in the scope of our research. The fourth iteration comprised an extensive screening of the abstract, which led to discarding additional 100 papers that were not relevant to the ROs. The abstract screening was performed on the papers that, based on the title, illustrated a potential link with our ROs, However the abstract conveyed information that differed from our ROs. This reduced the total number of papers to 65. The fifth iteration of our literature analysis consisted of eliminating papers due to lack of access. This iteration shrank the number of germane papers to 62. In the sixth step, a considerable scrutiny of the entire papers was executed to determine whether the papers were relevant to our ROs. The screening of the entire papers enabled us to articulately infer which papers were affecting our ROs. Papers lacking a clear specification of interfaces, or whose main focus moved from the data sharing processes were excluded, whereas the papers emphasizing interfaces and data sharing processes were included in the analysis. This iteration led to further filtering the number to 45 papers.

After rigorous consideration of the references in the 45 papers obtained by the sixth iteration, we applied backward search, restricted to the year 2010 the earliest, and forward search following vom Brocke et al. (2009), which produced a number increase of 16 papers. Hence, we encompassed a total of 61 adequate papers in our study.

The result set of the 589 papers after removing duplicates and non-English language papers at the beginning of the screening phase, plus the papers added from backward and forward search, 16, is available online as appendix containing 605 papers in total.[1]

3 Review of Interfaces for Implementation in Data Trusts

The concept of Data Trusts implies the usage of different types of interfaces (Table 1).

Table 1. Overview of Interfaces and Use Cases in Data Trust Ecosystems

	Interface Type (*Technologies*)	**Description** (*example use cases*)
Human-System Interf. (*User Interf.*)	Graphical User Interface (GUI)	A visual interface that allows data actors to interact with the Data Trust through structured elements such as forms, dashboards, icons, and menus, either native (desktop/mobile) or web-based (e.g., *consent management, access review, policy editing, data usage dashboard*)
	Web-Based Interface (e.g., *HTTP, HTML, CSS*)	A specific type of GUI delivered via standard web technologies and accessed through web browsers over HTTP / HTTPS (e.g., *browser-based user portal, consent portal, access requests, policy dashboard*)
	Data Visualization Interface (e.g., *D3.js, Apache Superset, Vega, Grafana*)	Interface for visualizing and monitoring dataset properties, usage metrics, and system flows through customizable dashboards and graphical representations (e.g., *data quality monitoring, usage analytics, lineage tracking dashboards*)
	Command-Line Interface (CLI) (e.g., *shell or terminal*)	Text-based interface for executing administrative tasks, scripting, and automation by entering commands directly into a terminal environment (e.g., *policy and access rules configuration, data pipeline deployment, system monitoring*)
System-System Interf. (*Tech. Interf.*)	Application Programming Interface (API) (e.g., *REST, GraphQL, gRPC*)	Programmatic interface that enables system interoperability for data exchange and workflow automation, locally or across platforms and networks (e.g., *dataset access, metadata queries, policy enforcement, identity and access management, audit logging, consent handling*)
	Representational State Transfer Interface (e.g., *HTTPS, JSON*)	A type of API that adheres to the REST architectural style, enabling stateless and secure data exchange using standard web protocols. (e.g., *dataset retrieval, user authorization, policy and consent updates*)
	Data Service Interface (e.g., *ETL protocols*)	Interface exposing operational data services to support data lifecycle management, including transformation and compliance-related processes (e.g., *data extraction, transformation and loading, policy validation, data synchronization*)
	Messaging or Streaming Interface (e.g., *Kafka, MQTT, AMQP*)	Interface for real-time or batch-based delivery of high-volume or asynchronous data, status updates, and event-driven messages (e.g., *event notifications, data streams, telemetry*)

[1] Dataset available from Acev et al. (2025) via zenodo.org

In the analyzed literature, some authors describe interfaces that are incorporated in Data Trusts explicitly. Others refer to the interfaces in a general sense without specifying any implementation in Data Trusts. We have considered papers that encompass types of interfaces that are important for the implementation of Data Trusts, regardless of whether the authors provide their direct implementation in Data Trusts.

Table 1 represents a summary of the interfaces found in the identified scholarly papers. The left-most column groups the interfaces into two main categories: human-system interfaces (user interfaces) and system-system interfaces (technical interfaces). The 'Interface Type (Technologies)' column, lists the interfaces found in the scholarly papers along with the technologies used to implement the interfaces. We establish the interface terms to be descriptive for future reference in Data Trusts, not how the authors refer to them in their studies. The 'Description (example use cases)' column provides a brief description of the corresponding interfaces as well as exemplary use cases tailored to Data Trusts.

The used terms for human-system interfaces in literature are: graphic user interface (GUI), web-based interface, data visualization interface, and command-line interface (CLI). The used terms for system-system interfaces in literature are: application programming interface (API), representational state transfer interface, data service interface, and messaging or streaming interface. In the following sub-sections, we elaborate on these *human-system* and *system-system interfaces* along with the indications of the references to the scholarly works.

3.1 Human-System Interfaces for Data Trusts

To meet the requirements of the data trust implementation, it is necessary to understand the human-system interaction. Many scholars argue that the user interfaces reflect on this incumbent human-system interaction as a requisite step in fulfilling Data Trusts (Lomotey et al., 2022; Patrick & Budd, 2010; Schinke et al., 2023). This reasoning translates to the establishment of a communication link between different data actors (e.g., data subjects, data owners, data providers, data consumers) and the Data Trust through a user interface (Musa et al., 2023; Schinke et al., 2023). The user interface provides several features, where the actors are encouraged to select the reason why they intended to communicate with the Data Trust initially in a user-friendly and efficient manner (Musa et al., 2023).

We faced challenges to clearly distinguish and define the human-system interfaces that are encompassed in literature, since they lack concretization. The term 'user interface' is used predominantly in several publications without any specification (Lähteenoja, 2023; Musa et al., 2023; Schinke et al., 2023; Sim et al., 2023). Musa et al. (2023) elaborate on the user interface as one of their blockchain-based framework's layers that serves as a bridge between the functionality of web applications and end-users, permitting the end-users to extract the benefits from the web application. Moreover, Schinke et al. (2023) state the necessity to provide a user interface as a web application, since it does not require data actors to install any specific software on devices to access the Data Trust. The authors further argue that for finding and accessing the pertinent data by human actors, a data marketplace represents an important component

(Schinke et al., 2023). The data marketplace relies on the user interface from a frontend perspective, whereas from a backend perspective it relies on the (meta)data broker, which allows appropriate searches for metadata or just data, and on vocabularies to prevent misunderstandings by offering user-specific data and service descriptions (Schinke et al., 2023). The features that are available to the actors need to be restricted and supported by rights and regulatory management, so the personal and other sensitive data remain strictly controlled (Sim et al., 2023).

Another term that appears in the literature is *GUI*. Essentially, a GUI is a part of user interfaces, where the data actors interact with the Data Trust using adapted graphics like designed icons and fields. Azcoitia & Laoutaris (2022) state that the data providers dispense data through a GUI, which facilitates the visual representation of the available features. Patrick & Budd (2010) present a Data Trust in the field of health industry, where an interface generator is accountable for creating the GUI the clinicians communicate with.

Web-based interfaces are not perspicuously described in the available literature. A web-based interface permits the data actors to interact with software running in the Data Trust via web browser. However, the accessible publications fail to demonstrate this relation in more details in the implementation of Data Trusts. Lomotey et al. (2022) demonstrate the Data Trust as a Service, where the authors elaborate on the connection between the web interface and presentation layer, which is a module that tackles all data actors' activities (e.g., routing requests, re-directing responses, and pushing notifications to other actors), through an HTTP/S communication protocol. Other authors just introduce the term "web interface" as a part of their Data Trusts without establishing a proper link between the frontend and the backend implementation for the web interface (Hildebrandt et al., 2020; Sayeed et al., 2023).

Data visualization interfaces are among the general user interfaces. The difference between the data visualization interface and GUI is slight. In fact, a data visualization interface can be considered as a user interface, where the data actors can monitor and visualize the characteristics of certain datasets. Qi et al. (2023) design an application layer that provides management services of data for industrial internet identity analysis for various industries like manufacturing, construction, consumer goods, food, agriculture and other industries through a visualization interface. Jha et al. (2022) present a novel framework for run-time trust state analyses of a virtual machine, where the interface shows several state information. Depending on the current system state, proper actions are triggered. In their cloud-based platform, Lomotey et al. (2022) implement a visualization interface to analyze data sharing workflows in a multi-partner environment. With this implementation, Lomotey et al. (2022) empower the actors to track their data along the data sharing process, and in doing so, they enhance transparency.

Command Line Interface (CLI) is briefly mentioned in the available literature. It lacks clear explanation especially in the realm of Data Trusts. While CLI refers to human-system interaction, it differentiates from the GUI through the course of action the data actors need to perform to realize the interaction. CLI allows data actors to interact with the Data Trust by typing commands directly into a terminal to operate. From the scarce explanation of literature in CLI implementation, Mehboob Khan et al. (2023) state that in their blockchain platform, the interaction with the actors is represented by a straightforward CLI, which triggers supporting APIs suitable for handling blockchain transactions. Shahbazi & Byan (2021) merely mention that CLI is part of their platform that is connected with a hyperledger composer REST server to generate REST APIs.

Overall, the human-system interfaces discussed in literature lack specifications of the implementation in Data Trusts, and they have not been rigorously studied yet, which implies the need to be meticulously studied in the future. It is crucial to point out that only a handful of authors discuss user interfaces in Data Trusts (Lomotey et al., 2022; Patrick & Budd, 2010; Sayeed et al., 2023; Schinke et al., 2023; Shahbazi & Byun, 2021), while others talk about the human-system interfaces without any specification in Data Trusts (Azcoitia & Laoutaris, 2022; Gruson-Daniel et al., 2023; Hildebrandt et al., 2020; Jha et al., 2022; Lähteenoja, 2023; Mehboob Khan et al., 2023; Musa et al., 2023; Qi et al., 2023; Sim et al., 2023). Although the implementation of different human-system interfaces varies from one field to another, it is important to stress that these interfaces have to be easily accessible and understandable to the data actors to facilitate the data sharing process and to stimulate human-system interaction. As such, the user interfaces represent a stepping stone in fully building Data Trusts.

3.2 System-System Interfaces for Data Trusts

Another interaction vital for the realization of the data trust ecosystem is system-system interaction. The system-system interaction reflects on the data transmission of information between inner components (different mechanisms) in the Data Trust, or between the Data Trust and other external systems (e.g., from other data intermediaries) (Abraham et al., 2019; Young et al., 2019). Technical interfaces translate to the system-system interaction in achieving Data Trusts (Bühler et al., 2023; Richter, 2023; Sayeed et al., 2023; Schinke et al., 2023; Specht-Riemenschneider & Kerber, 2022; Steinert & Altendeitering, 2024). The system-system policy guides automated system-system interactions, which eventually supplies the data actors or other entities (e.g., other organizations) with pertinent data via the data sharing process (Cohen et al., 2014).

Similar to the human-system interfaces, the system-system interfaces encompassed in literature demonstrate scarcity in explanation and implementation. This results in challenges to mark a clear difference and precision in defining the compulsory system-system interfaces in the construction of Data Trusts. The general term ‘technical interface’ is found in some publications without further detailed explication of the implementation and usage procedures (Jussen et al., 2024; Lähteenoja, 2023; Specht-Riemenschneider & Kerber, 2022). Lähteenoja (2023) specifies that technical interfaces for data providers differ from the technical interfaces for data recipients in technological aspects. Specht-Riemenschneider & Kerber (2022) present the necessity for standardized interoperable technical interfaces to enhance the interoperability and trustworthiness in the data trust ecosystem.

The most commonly used term in literature is *Application Programming Interface (API)*. From a technological aspect, APIs form the main interface for dealing and arranging actions between different applications, locally or over the network, by authorizing software programs to interact with each other in activities related to data (e.g., consumption, adding, processing, modification, or deletion of data) (Gruson-Daniel et al., 2023). APIs facilitate data discovery and stimulate data collaboration between desirable actors (Gupta & Panagiotopoulos, 2019). Implemented data sharing governance mechanisms include APIs, which facilitate a centralized data sharing within a data trust ecosystem (Micheli et al., 2020). Actors in the data trust ecosystem should have access to fully governed, standardized, and trustworthy APIs (Specht-Riemenschneider & Kerber, 2022; Steinert & Altendeitering, 2024). By applying these governance mechanisms and standards, the data trust augments the efficiency, technological capabilities, actors' capacities, and digital transformation of SMEs (Bühler et al., 2023).

Potential pitfalls from the implementation of APIs are, for instance, mentioned in Azcoitia & Laoutaris (2022). The authors argue challenges in the construction of data marketplaces for data sharing due to the severe implementation of access protocols or APIs in the system-system interaction. The convoluted connectivity interfaces could potentially undermine the performance of the organization; therefore, to avoid losses and breaches of data, there is a need for enhanced cybersecurity measures (Kifor & Popescu, 2024). To overcome these challenges, Azcoitia & Laoutaris (2022) propose that data marketplaces should set interoperability standards to combine APIs and produce a uniform way of accessing their data through an organization that mitigates the complexity of accessing data and that increases data's transparency.

Although existing literature provides an overview of APIs, their security measures, and their potential challenges, the literature lacks a studious elaboration on different types of APIs that could be incorporated in Data Trusts. With an exception of REST API, the of other types of APIs (e.g., Simple Object Access Protocol (SOAP), Remote Procedure Calls using XML (XML-RPC), etc.) are overlooked in Data Trust literature. In current literature on Data Trusts, APIs and REST APIs are mostly implemented in distributed ledger technologies (predominantly in blockchain), or digital twins (Lomotey et al., 2022, 2024; Shahbazi & Byun, 2021; Vilas-Boas et al., 2023). The exception is the Data Trust proposed by Steinert & Altendeitering (2024), where the authors present extensions to the Eclipse Dataspace Components (EDC). EDC is a compendious framework that states a fundamental set of features that can be reused and adjusted in dataspace implementations by implementing APIs and guaranteeing interoperability by design. Their extensions include Data Trusts incorporated in the dataspace ecosystem. To achieve these extensions, the EDC integrates a web server, which hosts a collection of public RESTful API endpoints (Steinert & Altendeitering, 2024). These endpoints of the extensions are integrated to manage the selection of a mutually trusted entity within the data space, from commencing and proceeding with the choice of a relevant Data Trust to informing the selected Data Trust for the data sharing process (Steinert & Altendeitering, 2024). Lomotey et al. (2024) stimulate the system-system communication in Data Trusts by introducing an API management system that is exposed as a RESTful endpoint, which is responsible for all system-system interactions.

Current literature lacks explanation of the term '*service interface*'. A service interface is an interface deployed to invoke a service. A generic understanding of data service interface in the realm of Data Trusts is provided by Schinke et al. (2023), where the authors refer to data service interface as a consequence of data actors' user request. They argue that the data service interface applies supporting protocols to explicitly interact with the entity or to yield a backend for the user interface (Schinke et al., 2023).

Messaging or streaming interface is depicted by Lomotey et al. (2022) in the presentation layer, which handles activities to the participants such as routing requests, redirecting responses, and pushing notifications. The authors elaborate on a notification mechanism to allow spreading of real-time information to a particular data actor (Lomotey et al., 2022). To be notified, each data actor has to register or subscribe based on a publisher-subscriber model (Lomotey et al., 2022).

The technical interfaces represent the driving mechanisms of the system-system interaction in the data trust ecosystem. A number of publications refer to the implementation in Data Trusts (Bühler et al., 2023; Jussen et al., 2024; Lomotey et al., 2022, 2024; Micheli et al., 2020; Potoczny-Jones et al., 2019; Richter, 2023; Sayeed et al., 2023; Schinke et al., 2023; Shahbazi & Byun, 2021; Specht-Riemenschneider & Kerber, 2022; Steinert & Altendeitering, 2024; Young et al., 2019). However, others do not specify an implementation in Data Trusts (Azcoitia & Laoutaris, 2022; Benzaïd et al., 2021; Borgogno & Colangelo, 2019; Cohen et al., 2014; Grechkin et al., 2017; Gruson-Daniel et al., 2023; Gupta & Panagiotopoulos, 2019; Hildebrandt et al., 2020; Jha et al., 2022; Kumar S. & Dakshayini, 2020; Lähteenoja, 2023; Mehboob Khan et al., 2023; Vilas-Boas et al., 2023). The realization of the system-system interfaces needs to be in accordance with the norms and regulatory standards to satisfy the data workflow and to ensure valuable system-system interaction within the data trust ecosystem.

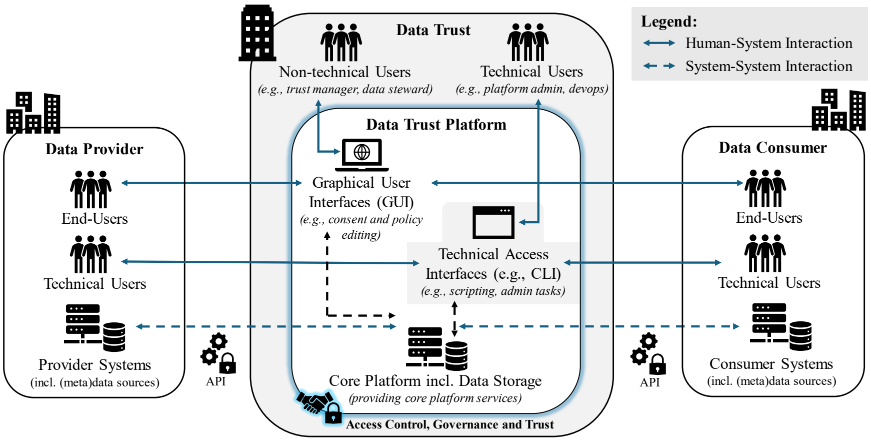
Legend:
Human-System Interaction
System-System Interaction
Data Trust
Non-technical Users
(e.g., trust manager, data steward)
Technical Users
(e.g., platform admin, devops)
Data Trust Platform
Data Provider
End-Users
Technical Users
Provider Systems
(incl. (meta)data sources)
API
Graphical User Interfaces (GUI)
(e.g., consent and policy editing)
Technical Access Interfaces (e.g., CLI)
(e.g., scripting, admin tasks)
Core Platform incl. Data Storage
(providing core platform services)
Access Control, Governance and Trust
Data Consumer
End-Users
Technical Users
Consumer Systems
(incl. (meta)data sources)
API

Figure 2. Human-System and System-System Interfaces in a Data Trust Ecosystem

To sum up, the human-system and system-system interfaces are prerequisites for the implementation of Data Trusts. Both groups of interfaces contribute uniquely to the achievement of seamless data sharing in the data trust ecosystem. Figure 2 represents the differences between the interfaces and how each interaction affects certain processes in the data trust ecosystem. The distinction of interfaces in the data trust ecosystem is vital for achieving smooth data sharing.

The literature analysis eminently addresses our RO1 by thoroughly investigating the current research on interfaces that are or can be implemented in Data Trusts. Our research also unveils that this field needs more studious work, especially when interfaces need to be implemented in data trust ecosystem. There are obvious gaps in existing literature that need to be tackled with focus. The next section therefore investigates types of data structures and the interfaces to the data sources.

4 Types of Data Structures and Interaction with Data Sources

To extract the full potential of the implemented interfaces, Data Trusts have to be designed to handle different data structures, and to link with storage implementations impeccably. In the following sub-sections, we analyze the structure of transmitted data through Data Trusts, and the interaction with the data sources.

4.1 Types of Data Structures

Data Trusts need to be capable of working with different structures of data, namely, semi-structured data like JavaScript Object Notation (JSON), unstructured data like images and documents, as well as with structured data as stored in relational databases (Potoczny-Jones et al., 2019). A de-facto standard for technical interfaces is the semi-structured JSON, which permits compatibility and interoperability across different types of systems (Potoczny-Jones et al., 2019). Shahbazi & Byun (2021) also utilize JSON data format for the acquisition of IoT sensor data that are later sent to a Kafka server. Lomotey et al. (2022) explain that in their blockchain-based Data Trust as a Service, REST APIs and JSON/Remote Procedure Call (RPC) protocol are used to interact with the deployed smart contracts. While JSON is widely adapted in literature, other standards like XML-RPC, SOAP and others are neglected, though.

To satisfy the heterogeneity of data, Young et al. (2019) construct a detailed data management architecture with coupled tiers: (1) A triage tier for unstructured data where raw files are ingested. This tier does not provide analysis capabilities. However, it offers secure and policy protected storage. It is implemented as a policy, authentication, and auditing layer; (2) a scalable data lake tier for semi-structured data utilized for quality control, analysis, restructuring, and integration where data can be infiltrated explicitly from the data providers; (3) a warehouse tier for structured data, where data can be absorbed directly through managed APIs, which ensures structured data management and imposes integrity constraints. All tiers are applied as administrative layers on top of existing cloud services (Young et al., 2019).

4.2 Interaction with Data Sources

Many potential data actors in the data trust ecosystem are incapable of hosting the data on premise and of ensuring continuous access to them. Thus, the data provided by the data providers need to be adequately stored in databases or other data sources, and secured for subsequent usage by the data users (Schinke et al., 2023). To attain this, Data Trusts need to provide APIs to existing services with storing functionalities, i.e. data sources, within its implementation (Schinke et al., 2023). A cloud storage allows an assembly of large amounts of data, security, and backups (Potoczny-Jones et al., 2019).

Data provenance is important in tracking the origins of the data. It should be saved in a relevant storage as well (Mehboob Khan et al., 2023).

Sayeed et al. (2023) provide a Data Trust, which assembles data from various interdisciplinary, geographically distributed databases. They create a multi-layered distributed database federation, where an access token is needed to access a database. Once the access token of the API is obtained, the access is gained (Sayeed et al., 2023).

Most of the publications refer to the types of databases installed in the data trust ecosystem (Potoczny-Jones et al., 2019; Shahbazi & Byun, 2021; Young et al., 2019). However, only a few of them elaborate on the APIs that need to be integrated to access or to provide data in the databases (Sayeed et al., 2023; Schinke et al., 2023). This illustrates another domain that requires attention and more extensive research.

By identifying existing mechanisms for accessing different data structures and providing links to databases in the data trust ecosystem, RO2 is fulfilled. Although there are exceptions (Lomotey et al., 2022; Young et al., 2019), the current literature conveys deficiencies in providing a thorough link between APIs and the available data structures. Moreover, there is a lack of detailed elaboration on the standards that can be used for the implemented interfaces in Data Trusts. The gaps in research can be observed in the interaction with data sources, where corresponding data is stored. Even though there is a strong base in some studies (Sayeed et al., 2023; Schinke et al., 2023), there is an apparent lack of designed APIs for the purpose of ensuring a smooth data flow to and from the data sources in the data trust ecosystem.

5 Research Gaps and Future Directions

Our systematic literature analysis identified significant research gaps. The different interface terms used in the analyzed publications lack a clear explanation. Hence, the general understanding of some terms may overlap, which conveys additional ambiguity among readers. Our work addresses this gap by systematizing and segregating the discussed interfaces in two main groups along with a provision of a common understanding of human-system and system-system interactions in a data trust ecosystem.

The evident lack of studious work in the system-system interaction uncovers the need for standards for APIs and user interfaces in Data Trusts to deal with different data structures. This lack increases when screening the literature on the interaction with databases, as there are barely papers that incorporate APIs to access data from and to provide data to the storage implementations of Data Trusts.

Existing literature conveys limited empirical validation of data trust models in specific domains, and insufficient research on interface design in the sphere of Data Trusts. This deficiency is due to the lack of scientific works referring to interface implementations in the data trust ecosystem. The current studies also lack interviews with non-expert and expert stakeholders, which restricts the stakeholder knowledge about the impact of human-system and system-system interaction along the data sharing process.

The deficiency of including cross-border or jurisdictional challenges in data trust implementations is evident, as well as the lack of standardized implementation of a universal framework for Data Trusts that complies with the data governance principles.

Through the performed systematic literature review, our research establishes the scientific grounds for developing human-system and system-system interfaces tailored to Data Trusts by highlighting the main contributions from current literature and the gaps that need to be tackled to set a solid and fiduciary data trust ecosystem. Thus, our study reveals the theoretical grasp of interfaces and their crucial implementation in Data Trusts. The implementation of these interfaces is a convoluted, yet a vital step in the construction of Data Trusts. Our work serves as a foundation for further technological developments, and practical implementation of the interfaces in data trust ecosystems.

For more concrete developments, future hands-on improvements have to be met for more practical implementations of the previously scrutinized interfaces. While our study does not provide an implementation of the discussed interfaces, we set the base for their construction by elaborating on the commensurable concepts.

6 Conclusion

In our work, we studied the field of Data Trusts and the interfaces utilized for achieving seamless fiduciary data sharing in the data trust ecosystem between the data actors and Data Trusts on a human-system and a system-system interface level. To achieve our ROs, we analyzed the current state of available literature on interfaces in Data Trusts.

By examining the current literature on this topic, we tackled RO1 as presented in Section 3, where we provide a comprehensive table of the relevant human-system and system-system interfaces, which are indispensable for building Data Trusts. The widespread imprecision in defining and addressing these interfaces makes it strenuous to implement interoperable interfaces in the construction of Data Trusts.

A clearer understanding of the necessary interfaces allows a smooth data flow in the data sharing process. However, to design robust Data Trusts, other mechanisms need to be taken into consideration as well. Data Trusts need to be able to interact with different structures of data (e.g., unstructured, semi-structured, and structured data), and they need to provide an interface to and from the databases. By examining the existing literature in Data Trusts' interfaces, determining the deficiencies and the existing gaps, we successfully tackle RO2 and present our standpoint in Section 4.

This work is merely a primary step in our ultimate objective, to construct a functionable fiduciary Data Trust with strong user and technical interfaces integrated accordingly to enhance flawless data sharing processes between various entities. Our future work in our projects "EG-DAS" and "KOOP-DAS"[2] will focus on the practical implementation and demonstration of operation of the interfaces in data trust ecosystems.

Acknowledgements

This research has been supported by the Federal Ministry of Research, Technology and Space (BMFTR), Germany under Research Grants No. 16DTM218 and 16DTM411A as part of the NextGenerationEU program of the European Union.

[2] More information available from https://datentreuhandschaft.de/

References

Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, *49*, 424–438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Acev, D., Rieder, F., Riehle, D. M., & Wimmer, M. A. (2025). *Supplementary Dataset: Systematizing Different Types of Interfaces to Interact with Data Trusts* [Dataset]. Zenodo. https://doi.org/10.5281/zenodo.15704523

Austin, L. M., & Lie, D. (2021). Data Trusts and the Governance of Smart Environments: Lessons from the Failure of Sidewalk Labs' Urban Data Trust. *Surveillance & Society*, *19*(2), 255–261. Publicly Available Content Database. https://doi.org/10.24908/ss.v19i2.14409

Ayappane, B., Vaidyanathan, R., Srinivasa, S., Upadhyaya, S. K., & Vivek, S. (2024). Consent Service Architecture for Policy-Based Consent Management in Data Trusts. *ACM Int. Conf. Proc. Ser.*, 155–163. Scopus. https://doi.org/10.1145/3632410.3632415

Azcoitia, S. A., & Laoutaris, N. (2022). A Survey of Data Marketplaces and Their Business Models. *SIGMOD Rec.*, *51*(3), 18–29. https://doi.org/10.1145/3572751.3572755

Benzaïd, C., Taleb, T., & Farooqi, M. Z. (2021). Trust in 5G and Beyond Networks. *IEEE Network*, *35*(3), 212–222. IEEE Network. https://doi.org/10.1109/MNET.011.2000508

Borgogno, O., & Colangelo, G. (2019). Data sharing and interoperability: Fostering innovation and competition through APIs. *Computer Law & Security Review*, *35*(5), 105314. https://doi.org/10.1016/j.clsr.2019.03.008

Bühler, M. M., Calzada, I., Cane, I., Jelinek, T., Kapoor, A., Mannan, M., Mehta, S., Mookerje, V., Nübel, K., Pentland, A., Scholz, T., Siddarth, D., Tait, J., Vaitla, B., & Zhu, J. (2023). Unlocking the Power of Digital Commons: Data Cooperatives as a Pathway for Data Sovereign, Innovative and Equitable Digital Communities. *Digital*, *3*(3), 146. Coronavirus Research Database; Publicly Available Content Database. https://doi.org/10.3390/digital3030011

Cohen, S., Money, W., & Quick, M. (2014). Improving Integration and Insight in Smart Cities with Policy and Trust. *Proceedings of the 4th International Conference on Web Intelligence, Mining and Semantics (WIMS14)*, 1–9. https://doi.org/10.1145/2611040.2611091

European Commission. (2017). *Communitcation from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – European Interoperability Framework (EIF) – Implementation Strategy.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017DC0134

Feth, D., & Rauch, B. (2024). Datentreuhänder in der Praxis. *Datenschutz und Datensicherheit - DuD*, *48*(2), 103–109. https://doi.org/10.1007/s11623-023-1889-3

Grechkin, M., Poon, H., & Howe, B. (2017). Wide-Open: Accelerating public data release by automating detection of overdue datasets. *PLOS Biology*, *15*(6), e2002477. https://doi.org/10.1371/journal.pbio.2002477

Gruson-Daniel, C., Jean, B., Medjaoui, M., & Boyd, M. (2023). *Improving Trustworthy and Sustainability Digital Infrastructures with The Fair API Commitment to Trust Model* (p. 88). Inno3 ; Les mainteneurs ; Platformable. https://hal.science/hal-04180319

Gupta, A., & Panagiotopoulos, P. (2019). Operational Capabilities for Smart City Data Management. *Proceedings of the 20th Annual International Conference on Digital Government Research*, 504–506. https://doi.org/10.1145/3325112.3328215

Hildebrandt, K., Panse, F., Wilcke, N., & Ritter, N. (2020). Large-Scale Data Pollution with Apache Spark. *IEEE Transactions on Big Data*, *6*(2), 396–411. IEEE Transactions on Big Data. https://doi.org/10.1109/TBDATA.2016.2637378

Jha, D. N., Lenton, G., Asker, J., Blundell, D., & Wallom, D. (2022). TrustedCloud: A framework for the run-time trust state analysis of a virtual machine in cloud environment: demo abstract. *Proceedings of the 23rd International Middleware Conference Demos and Posters*, 17–18. https://doi.org/10.1145/3565386.3565492

Jussen, I., Möller, F., Schweihoff, J., Gieß, A., Giussani, G., & Otto, B. (2024). Issues in inter-organizational data sharing: Findings from practice and research challenges. *Data & Knowledge Engineering*, *150*, 102280. https://doi.org/10.1016/j.datak.2024.102280

Kifor, C. V., & Popescu, A. (2024). Automotive Cybersecurity: A Survey on Frameworks, Standards, and Testing and Monitoring Technologies. *Sensors*, *24*(18), Article 18. https://doi.org/10.3390/s24186139

Kumar S., N., & Dakshayini, M. (2020). Secure Sharing of Health Data Using Hyperledger Fabric Based on Blockchain Technology. *2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI)*, 1–5. https://doi.org/10.23919/ICOMBI48604.2020.9203442

Lähteenoja, V. (2023). What are “personal data spaces”? *Companion Proceedings of the ACM Web Conference 2023*, 1458–1461. https://doi.org/10.1145/3543873.3587656

Lis, D., Gelhaar, J., & Otto, B. (2023). Data Strategy and Policies: The Role of Data Governance in Data Ecosystems. In I. Caballero & M. Piattini (Eds.), *Data Governance: From the Fundamentals to Real Cases* (pp. 27–55). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-43773-1_2

Lomotey, R. K., Kumi, S., & Deters, R. (2022). Data Trusts as a Service: Providing a platform for multi-party data sharing. *International Journal of Information Management Data Insights*, *2*, 100075. https://doi.org/10.1016/j.jjimei.2022.100075

Lomotey, R. K., Kumi, S., Ray, M., & Deters, R. (2024). Synthetic Data Digital Twins and Data Trusts Control for Privacy in Health Data Sharing. *Proceedings of the 2024 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems*, 1–10. https://doi.org/10.1145/3643650.3658605

Mehboob Khan, K., Haider, W., Ahmed Khan, N., & Saleem, D. (2023). Big Data Provenance Using Blockchain for Qualitative Analytics via Machine Learning&nbsp; *JUCS - Journal of Universal Computer Science*, *29*(5), 446–469. https://doi.org/10.3897/jucs.93533

Micheli, M., Ponti, M., Craglia, M., & Berti Suman, A. (2020). Emerging models of data governance in the age of datafication. *Big Data & Society*, *7*(2), 2053951720948087. https://doi.org/10.1177/2053951720948087

Mohamed, M. A., Galal-Edeen, G. H., Hassan, H. A., & Hasanien, E. E. (2012). An evaluation of enterprise architecture frameworks for e-government. *2012 Seventh International Conference on Computer Engineering & Systems (ICCES)*, 255–260. https://doi.org/10.1109/ICCES.2012.6408524

Musa, H. S., Krichen, M., Altun, A. A., & Ammi, M. (2023). Survey on Blockchain-Based Data Storage Security for Android Mobile Applications. *Sensors*, *23*(21), Article 21. https://doi.org/10.3390/s23218749

O’Hara, K. (2019). *Data trusts: Ethics, architecture and governance for trustworthy data stewardship*. http://dx.doi.org/10.5258/SOTON/WSI-WP001

Otto, B., & Jarke, M. (2019). Designing a multi-sided data platform: Findings from the International Data Spaces case. *Electronic Markets*, *29*(4), 561–580. https://doi.org/10.1007/s12525-019-00362-x

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S.,

… Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, n71. https://doi.org/10.1136/bmj.n71

Panian, Z. (2010). Some Practical Experiences in Data Governance. *World Academy of Science, Engineering and Technology*, *62*.

Patrick, J. D., & Budd, P. (2010). Ockham's razor of design: An heuristic for guiding design and development of a clinical information systems generator. *Proceedings of the 1st ACM International Health Informatics Symposium*, 18–27. https://doi.org/10.1145/1882992.1882998

Potoczny-Jones, I., Kenneally, E., & Ruffing, J. (2019). Encrypted Dataset Collaboration: Intelligent Privacy for Smart Cities. *Proceedings of the 2nd ACM/EIGSCC Symposium on Smart Cities and Communities*, 1–8. https://doi.org/10.1145/3357492.3358630

Qi, Z., Huang, T., Zhang, B., Li, Y., & Zhang, X. (2023). Research on Trusted Management of Industrial Internet Identity Analysis Data Based on Blockchain. *Symmetry*, *15*(12), Article 12. https://doi.org/10.3390/sym15122102

Richter, H. (2023). Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing. *GRUR International*, *72*(5), 458–470. Scopus. https://doi.org/10.1093/grurint/ikad014

Rowe, F. (2014). What literature review is not: Diversity, boundaries and recommendations. *European Journal of Information Systems*, *23*(3), 241–255. https://doi.org/10.1057/ejis.2014.7

Sayeed, S., Pitropakis, N., Buchanan, W. J., Markakis, E., Papatsaroucha, D., & Politis, I. (2023). TRUSTEE: Towards the creation of secure, trustworthy and privacy-preserving framework. *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 1–10. https://doi.org/10.1145/3600160.3604997

Schinke, L., Hoppen, M., Atanasyan, A., Gong, X., Heinze, F., Stollenwerk, K., & Roßmann, J. (2023). *Trustful Data Sharing in the Forest-based Sector—Opportunities and Challenges for a Data Trustee*. 49th International Conference on Very Large Data Bases (VLDBW'23), Vancouver, Canada.

Shahbazi, Z., & Byun, Y.-C. (2021). Smart Manufacturing Real-Time Analysis Based on Blockchain and Machine Learning Approaches. *Applied Sciences*, *11*(8), Article 8. https://doi.org/10.3390/app11083535

Sim, J., Kim, B., Jeon, K., Joo, M., Lim, J., Lee, J., & Choo, K.-K. R. (2023). Technical Requirements and Approaches in Personal Data Control. *ACM Comput. Surv.*, *55*(9), 190:1-190:30. https://doi.org/10.1145/3558766

Specht-Riemenschneider, L., & Kerber, W. (2022). *Designing Data Trustees—A Purpose-Based Approach*.

Stachon, M., Möller, F., Guggenberger, T., Tomczyk, M., & Henning, J.-L. (2023). Understanding Data Trusts. *ECIS*. Thirty-first European Conference on Information Systems (ECIS 2023), Kristiansand, Norway.

Steinert, M., & Altendeitering, M. (2024). Data Trustees: A Whitelisting Approach for Trusted Data Sharing. *Proceedings of the 4th Eclipse Security, AI, Architecture and Modelling Conference on Data Space*, 86–92. https://doi.org/10.1145/3685651.3685656

Vilas-Boas, J. L., Rodrigues, J. J. P. C., & Alberti, A. M. (2023). Convergence of Distributed Ledger Technologies with Digital Twins, IoT, and AI for fresh food logistics: Challenges and opportunities. *Journal of Industrial Information Integration*, *31*, 100393. https://doi.org/10.1016/j.jii.2022.100393

vom Brocke, J., Simons, A., Niehaves, B., Niehaves, B., Reimer, K., Plattfaut, R., & Cleven, A. (2009). *Reconstructing the giant: On the importance of rigour in documenting the literature search process*. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1145&context=ecis2009

vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., & 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*. https://doi.org/10.17705/1CAIS.03709

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), xiii–xxiii. http://www.jstor.org/stable/4132319

Young, M., Rodriguez, L., Keller, E., Sun, F., Sa, B., Whittington, J., & Howe, B. (2019). Beyond Open vs. Closed: Balancing Individual Privacy and Public Accountability in Data Sharing. *Proceedings of the Conference on Fairness, Accountability, and Transparency*, 191–200. https://doi.org/10.1145/3287560.3287577