Towards Robust Trust Frameworks for Data Exchange: A Multidisciplinary Inquiry

Aytaj Badirova [1], Bithin Alangot[2], Theo Dimitrakos[3], and Ramin Yahyapour[4]

Abstract: Data exchange is essential in the fast-changing field of data-driven innovations. In exploring the importance of data and data exchange, this paper highlights the necessity of building trust. For data sharing to be successful, trust is essential for assuring reliability, security, and ethical behaviour. We review the current state of the art where research and real-world applications converge in both academia and industry. Notably, trust framework-based projects are starting to take shape, promoting safe and open data markets that are included in this work. Nonetheless, challenges still exist, such as complex legal, technological, and business issues. Some of the main challenges that are faced while establishing a trust framework have also been briefly mentioned in this paper.

Keywords: trust framework, dataspace, data exchange

1 Introduction

Data is the cornerstone of innovations and a fundamental asset for organizations. A tremendous amount of data is being gathered and maintained. From business to health, each sector continuously gathers and maintains data, primarily internally and in accordance with local norms and regulations. On the other hand, interconnectivity is necessary to advance development in collaborative processes and innovations. The significance of data lies in the potential of bringing novelties. Data kept in silos cause different obstacles in various sectors creates a barrier for success in data exchange. The most frequent problems are those with trust, compliance (e.g., technical, legal, or policy level), and laws. The foundational prerequisite for the data exchange process is establishing an appropriate trust architecture that parties can adhere to. Encouraging a trustworthy framework will draw in a higher number of partners, increasing the volume and variety of data exchanged and broadening the scope. Trust architecture plays therefore a crucial role in data management and is a basement for innovations. To enable trust in a large data exchange where there are numerous participants from diverse backgrounds (e.g., different policies, access management schemas, or legal variations in

[1] German Research Center, Huawei Technologies Düsseldorf GmbH, Munich, Germany, email: aytaj.badirova@huawei.com,
[2] German Research Center, Huawei Technologies Düsseldorf GmbH, Munich, Germany, email: bithin.alangot@huawei.com
[3] School of Computing, University of Kent, Canterbury, UK, email: theo.dimitrakos@huawei.com
[4] Institute of Informatik, University of Goettingen, Goettingen, Germany, email: ramin.yahyapour@gwdg.de

doi:10.18420/OID2024_01

a case of cross-border collaborations) is a very challenging process, and to have an architecture that works for all is nearly unattainable. However, for an adequate number of participants with more similar interests, domain-specific trust can still be enabled. In order to address the aforementioned difficulties in establishing a trustworthy data exchange environment, Fraunhofer Institute developed a novel strategy known as Dataspace. The participants of a dataspace or dataspaces can publish and share their data with other participants in a secure way while being compliant with various regulations. Dataspace provides interconnectivity while encouraging data sovereignty – participants decide to give access to others in the ecosystem. The process of establishing such a system starts with trust. However, achieving a shared sense of trust without depending on a single, central decision-making authority is an incredibly challenging task. Though very difficult, a number of studies and projects aim to create a decentralised, unbiased, and equitable trust structure that can benefit all parties equally. One of the recent initiatives called the International Dataspace Association - IDSA [IDS24] is formed to support and govern the adoption of such a trustworthy environment. The role of IDSA is to coordinate and support the processes at a business level, however, there is still a need to define more granular approaches to define a secure architecture and guidelines. Gaia-X [Gai24] is another important initiative to foster data sovereignty, interoperability, and secure data exchange by providing reference architectures and trusted frameworks. Both initiatives have been covered in this report together with current implementations and projects where the main focus is establishing a trust framework that helps participants follow the EU's data strategy. Industry and academia propose diverse approaches for building domain-specific trust. This work aims to review the major models from different fields, both conceptual and practical with their pros and cons, and discuss the significant challenges that still need to be resolved.

This is the first thorough study of trust in a data exchange domain. The study's classification of various data exchange strategies into different categories according to their features, characteristics, and needs, such as industrial/international, cyber-threat intelligence, personal, and transportation dataspace models, is another significance distinction. Furthermore, by outlining potential benefits and flows, this paper questions the current solutions and offers valuable guidance for future research and ecosystem development.

2 Scholarly Foundations and Practical Implications

Although the process of exchanging data is not new, the idea of "dataspace" seeks to expand it into the direction of sovereign data. This data management approach focuses on uniting data/service providers under one roof and offering them a reliable, seamless infrastructure for data exchange while encouraging data sovereignty. In order to achieve its primary objective, there are several proposed approaches for data exchange architecture and to establish a trust framework to make the exchange process reliable in dataspace system. Scholarly foundations and the most prominent architectures and

frameworks have been explored together with leading initiatives in this section.

2.1 Trust in Data Exchange

To establish a reliable data sharing environment, proper data exchange mechanisms are crucial. Data exchange models provide a framework for defining the roles and responsibilities of the parties involved in data exchange, as well as the technical mechanisms for securely transferring and storing data. There is a slight gap between the state of the art in academics and industry, which is also influenced by strict regulations, given the rapid advancement of technology. At this point, it is important to note that the trust framework in dataspace is a very broad concept, and covering every component in a single study is quite difficult. Thus, the majority of the works that are suggested concentrate on a particular aspect of building trust. This section's first half discusses the state of research regardless of a particular domain, and the latter portion focuses on the state of the industry.

State of the Art in Research: Fraunhofer IAO suggested the Trust mAnagement Infrastructure (TRAIN) [Jey22] as a trust schema to build trust in decentralised identity data management. The suggested methodology provides a scalable mechanism to confirm the credential's issuer and determine its reliability. The DNS list serves as the foundation for both the model and the verification process. The proposed has approach many great benefits, but it also has several drawbacks, like being limited to a static list and missing a trust level variation. Establishing trust in a decentralized environment for identity data highly depends on the used technology on personal devices – so called digital wallets. There are relatively small amount of work that focuses on security in wallets such as the apporach called DOOR [La23]. The proposed model facilitates the establishment of both identity integration and wallet validity while being aligned with the current regulations (e.g., eIDAS). It applies Attribute-based Direct Anonymous Attestation (DAA-A) cryptographic protocol to ensure anonymity, unforgeability, and unlinkability.

Different sectors have diverse approaches when it comes to data sharing. The purpose of the article [CFH22] is to assess and examine common automotive HTAs (hardware trust anchors) in terms of their suitability for application in contemporary and future vehicle architectures. The authors use the automotive domain analysis and associated studies to establish thorough evaluation criteria in order to do this. Key technologies evaluated are Trusted Platform Module, Hardware Security Module, and Secure Hardware Extension. By bridging the gap between theoretical discussions and real-world requirements in the automotive arena, the study offers a thorough review of HTAs. Another study focuses on trust establishment for data exchange in the Internet of Vehicles (IoV)[AlM24]. It uses Naive Bayes machine learning to propose a classification-based trust model (CTM) that is specifically designed for IoV. By classifying cars as trusted or untrusted, this concept improves secure communication throughout the Internet of Vehicles. In the era of connected automobiles, the research advances safer data transmission by improving the

effectiveness of trusted and untrusted vehicle recognition.

In diverse ecosystems, the quantity of participants in data exchange may differ. Whether centralised or decentralised, the exchange procedure becomes increasingly difficult as the number of participants rises due to the variations in access control methods. It complicates the process of building trust. Thus, it is necessary to build a bridge between two different systems, especially between decentralised and legacy systems. The goal of the Fed2SSI [Ku23] suggested architecture is to build this bridge by converting legacy credentials into the appropriate verifiable presentation (VP), which is comprehensible to all parties involved in the data exchange ecosystem. The suggested method boosts participant trust while enhancing interoperability. The study [SSA21] focuses on a novel approach to data exchange that is inspired by Channel Island legislation. The main focus is on data governance and trust. The study aims to establish trust in personal data exchange by including citizens as stakeholders. The key guidelines have been proposed to implement them in practice for organizations. The guidelines define the boundaries, goals, stakeholders, limitations, and responsibilities. On the other hand, it has limitations, such as not covering diversities in trust levels and different data types.

Exploring Industrial Initiatives: IDSA and Gaia-X provide frameworks for trust establishment, negotiation, and data exchange. IDS-RAM [IDS24] is the initial data exchange framework that is provided by IDSA that is aligned with Gaia-X trust framework. The main component of the architecture is a Connector. In the secure dataspace formed by the Connector connection, the data provider and the data consumer transfer data including data metadata, data + usage policies, and data processed in the DataApp. Parties in an IDS can exchange data over secure channels using the IDS Communications Protocol (IDSCP).

The IDS-RAM data exchange model is primarily designed for industrial data and is not well-suited for personal data, which is more sensitive and requires a more privacy-focused approach. One such conceptual model is the W3C SOLID Data Pod [Sa16], a decentralized data storage system that gives users full control over their data. SOLID Data Pods offer advantages for personal data exchange, including decentralization, user control, and fine-grained access control. SOLID aims to provide private spheres – PODs for individuals to keep the control over their data. Instead of a centralized systems, the data can be stored in decentralized way. Users have full control of their data, they decide who can access what, to what degree.

Distributed Data Store Mesh is another proposed approach for securing personal data exchange process. It puts control over personal data governance, disclosure and usage in the hands of the data owner. These ledgers are well suitable for providing the immutable foundation for Decentralized Identifiers, but should not be used to store personal identity data. This would be at odds with the goals of privacy by design and with existing and emerging data regulations, such as the GDPR. Instead, we need a different solution for secure storage of personal data and information. Identity Hubs are that solution. Identity

Hubs are decentralized, off-chain, personal data stores that put control over personal data in the hands of users. They allow users to store their sensitive data-identity information, official documents, app data, etc.-in a way that prevents anyone from using their data without their explicit permission. Users can use their Identity Hubs to securely share their data with other people, apps, and businesses, providing access to the minimum amount of data necessary, while retaining a record of its use.

A significant portion of the data-focused industries are covered by industrial and personal dataspaces, but not nearly enough to address problems in other specialized industries, like transportation. To improve the transportation systems for passengers and transports the projects C3ISP [C324] and E-CORRIDOR [Ed24] established another data exchange framework that serves Collaborative Cyber Threat intelligence (C3IS). They employ a data exchange pattern that is based on the transfer of a bundle consisting of protected data and the associated agreement about sharing and usage of the protected data. This is referred to as Data Bundle or (Data Protected Object). Data exchange relies on Data Sharing Agreements (DSAs) to manage access and usage of data. Each DSA incorporates information about data provider, data consumer, the validity period of the DSA, a list of parties that can use this DSA and map it to their data and a set of policies.

The described models emphasise a secure method of data exchange. However, maintaining data control both during transmission and after exchange is a difficult challenge. Therefore, a new approach was proposed by MIT OPAL [Ce23] that focuses on moving algorithms, not data. Data needs to be stored in an encrypted form and computations should be done on the data side on encrypted data. OPAL ("Open Algorithms") is a non-profit social technology innovation founded in 2017 by the MIT Media Lab. The core idea is that data is not copied or moved. Algorithms are deployed on computing nodes of data providers after privacy compliance review – bring algorithm to data, not vice versa. The access control scheme in this concept is called consent for execution instead of consent for access.

The aforementioned architectures, which include the identity hub in distributed data mesh, the pod in W3C Solid, and the connector in IDS architecture, center on the flow of data exchange. These methods are insufficient on their own to provide a safe and reliable environment. It emphasizes the necessity of the trust frameworks where the primary dataspace trust frameworks have been covered in the next section.

2.2 Trust Frameworks

Sharing and accessing digital data is a way of building robust systems, and analytics, dealing with obstacles in business, and opening new horizons for organizations. Security is one of the key features of digital data sharing. Regardless of academia or industry, the goal is to share/access required data in a trustworthy way where the degree of security must be agreed upon. This agreement should be based on a set of rules – not only company-based, but also high level such as national and international. This systematic

collection of rules is called a Trust Framework. By enacting the necessary legislation and acts, the trust framework creates a reliable data sharing environment for all participants. A trust framework architecture has been initiated by many participants in the dataspace domain. This section covers the primary approaches. The Gaia-X Association developed its Gaia-X Framework, which enables the transition from disjoint data and infrastructure ecosystems, to composable, interoperable, and portable cross-sector data sets and services. Gaia-X Framework builds on top of the X-Model in order to enable trust and interoperability within and across dataspaces and federations. The Gaia-X Trust Framework is the set of rules that define the minimum baseline to be part of the Gaia-X Ecosystem. Those rules provide common governance and the basic level of interoperability across individual ecosystems while letting the users be in full control of their choices.

While Gaia-X offers a trust framework for specifically dataspace, Trust Over IP [Da19] trust model concentrates on internet-wide trust via verifiable credentials, trust registries, and decentralized identity. ToIP trust framework is supported by Linux Foundation. The goal is to provide a “trust layer” that can be achieved internet-wide. The model merges technology and governance in four layers of stack where the technology stack includes Public Utilities, Peer-to-Peer Communication, Trust Task Protocols, Application Ecosystem and the governance stack contains Utility Governance Framework, Agent/Wallet Governance Framework, Trust Tasks Framework, Ecosystem Governance Framework. The greater and more comprehensive scope of ToIP increases complexity and slows down the adaption process.

DSBA Trust Framework [DS24] is another trust model approach that provides a Trust Anchor for a secure ecosystem. DSBA Trust Anchor adopts Gaia-X Trust Framework and sets additional rules on top of it which allow organizations to use their digital identities for interactions. This makes it easier for organizations to trust each other and share data securely. DSBA trust framework focuses more on business compliance while previously mentioned approaches are technical compliance oriented. DSBA TF addresses he issues mentioned in Figure 1.

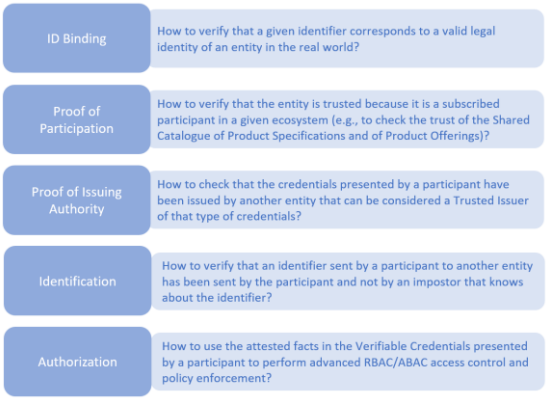

Figure 1 DSBA TF focused issues

Compared to other data types, the trust framework for identity data demands a more fine-grained and privacy-preserving trust architecture, especially in the EU. eIDAS [eID24] aims to provide a secure trust framework architecture for primarily identity data exchange in the EU among organizations, institutions, medical, and banking sectors etc. The goal is to make the digital identity available EU-wide. However, the concept is not limited to the EU, but can be adapted to other regions as well. The project supports the sovereign identity concept where individuals are in charge of their personal data, they should be able to share only the required data via a selective disclosure method and should be compatible with GDPR rules. An enhanced version of eIDAS, known as eIDAS2, was proposed in an effort to increase trustworthiness. Increased user experience, cross-border adaptability, and e-ID schema convergence are the goals of the new version. The trust frameworks that have been discussed encompass a variety of industries and data kinds. Overall, they all work toward the same objective of facilitating trustworthy and safe data transfers across the EU and beyond while abiding by national, international, and local laws and regulations. These architectures have been applied in the implementation of the initial dataspace projects that are discussed in detail in the following section. The first dataspace initiatives, which are covered in detail in the section that follows, were implemented using these architectures.

2.3 Initiatives and Trends

The design and acceptance of secure data exchange efforts across multiple industries and data sectors have been advocated for by a variety of public and commercial entities. Several notable initiatives by the main actors are covered in this section. Industrial/international dataspaces are designed for scalable enterprise data exchange and collaboration among businesses and organizations. They must handle a wide variety of structured and unstructured data, often at high volume and velocity. Industrial/international dataspaces provide robust data ingestion, processing,

management, and usage control mechanisms of the data based on commonly agreed policies. These are built to facilitate data exchange and collaboration at an industrial or organizational level. In these environments, data from various sources, including IoT devices, operational data, business data, etc., is pooled and made accessible to participating entities under specific conditions. The governance model in industrial dataspaces ensures a secure, controlled and equitable sharing of data, respecting data privacy laws, and facilitating collaboration and value creation. The typical data exchange pattern for industrial/international dataspace is that of an IDS connector architecture and the IDSA Dataspace Protocol. The emerging reference architecture for such dataspaces is based on a convergence of the IDS-RAM and the Gaia-X Architecture on a baseline defined by the DBSA convergence activity. Most of the current lighthouse projects follow this model. Catena-X [Cat24], German Mobility Dataspace (MDS) [MD24] and (more recently) Manufacturing-X [MX24] are the most widely recognized initiatives in this domain.

Mobility Dataspace is another striking dataspace idea that has drawn interest in the EU. Particularly, the German government is interested in developing this industry. More than 200 German mobile stakeholders from science, business, and public administration participated in its vision. Its goal is to further develop the Mobility Dataspace as a business organization and ensure its technological advancement. Traffic optimization, multimodal transportation, and new mobility services are among the main objectives of the Mobility Dataspace while establishing a sustainable, efficient, and user-friendly mobility system.

Intelligent Transportation System (ITS) Dataspaces and mobility dataspaces are designed to offer an open ecosystem that enables the trustworthy exchange of data between different traffic participants, providers, and operators in order to optimize traffic flows, increase safety and protect the environment. The ITS dataspace addresses use-cases that are related to data generated by vehicles, privately owned mobile devices, as well as may be collected and processed by public transport providers, navigation service providers, fleet operators (OEMs) and mobile communication providers (MNOs) which is of sensitive in nature and need to be handled uniquely (with separate policies and technical requirements).

Automotive and mobility dataspace schemas follow industrial data exchange patterns. However, this approach is insufficient for person data. Therefore, a new dataspace architecture model was established called Personal Dataspace. Personal Dataspaces are designed around individual users, enabling them to maintain control and portability over their own data, deciding who has access and for what purpose. The architecture of personal dataspaces usually prioritizes ease of use, transparency, and privacy. MyData Global [MG24] is the main forum where new projects focusing on personal dataspaces are concentrated. The typical characteristic of the dataspace is targeting specific data sectors such as industry, mobility, health, green hub etc. It brings out one of the main differences of personal dataspaces – to play a bridge role among dataspaces. aNewGovernance is one of those examples that focuses on this feature [AG24]. Its goal

is to move from platform-centric data model to human-centric one – individuals should be able to use their data on diverse dataspaces without additional adjustment. Since aNewGovernance targets personal data it has to follow GDPR and other personal data regulations strictly. Personal dataspace covers data more than personal identity information, such as skills and education. Dataspace for Skills (DS4Skills) [DS24] and Prometheus (from DASES - Dataspace Education and Skills) [Px24] both aim to collect, store, and securely share educational and skill data with businesses with the permission of data owners. Individuals will be able to quickly enter the job market in this way, while organizations will have better opportunities to locate skilled staff.

As of now, the presented dataspaces serve similar purposes such as increasing connectivity, establishing new business models, supporting business growth, encouraging sovereignty while preserving security. However, dataspace can also be established to increase security in digital ecosystem – preventing cyber-crimes. In this case, security is the goal not the feature. Sensitive Dataspaces (SDS) are designed with that goal in mind. Sensitive Dataspace's consists of building blocks that can help with secure storage, management, exchange and analysis of data of critical nature, such as cyber-incidents information and more detailed Cyber Threat Intelligence (CTI). As with any dataspace, SDS relies on a data governance paradigm, which comprises a set of rules and policies determining the rights to access process, use and share data in a trustful way. Since data used and shared within this particular dataspace is considered to be sensitive and contains confidential information, data providers must have complete control over who can have access to their data, for which purpose, and under which conditions it can be used. The C3ISP and CyCLONe projects [C324] project are of examples of a sensitive dataspace.

3 Challenges

A reliable data exchange ecosystem has given businesses new avenues for growth. Thus far, the present implementations and initiatives, together with the concept of dataspace and its primary characteristics and components, have been discussed. Nevertheless, like other advancements, it has its share of obstacles and challenges. This new strategy, given its infancy, presents a number of challenges and risks from many angles that need to be handled. To provide an overview, this section addresses the main challenges in the dataspace domain, ranging from technological to legal, business, and sectoral (Figure 1). Sovereign data management gives companies more control and security, but it also presents new difficulties. It takes a significant adjustment to create new business models that succeed in a decentralised data environment. Complexity is increased by creating and sustaining a dynamic network of cooperative partners. It might be difficult to negotiate data usage with different parties under different legislation. To fully realize the benefits of data sovereignty, businesses must carefully negotiate these obstacles, weighing opportunities against the reality of this shifting paradigm.

3.1 Domain Specific Challenges

Health: Health data is one of the most crucial data types that requires high security and privacy. Therefore EU aims to bring sovereignty to this data type where the individuals will be in full control of the data. The data sovereignty approach seems promising to prevent security incidents. Hence, it completely aligns with the first purpose of health data. However, when it comes to the secondary use of health data - which is research, the new approach creates barriers such as getting consent from users, translating the language of the data when changing the country, security of the shared data in the case of doctor visits etc. A more comprehensive evaluation of the security concerns related to health data has been covered in the study [Ma23]. These challenges call for an appropriate foundation of trust wherein the requirements of both sides of the health data can be met. The answer has not yet been developed.

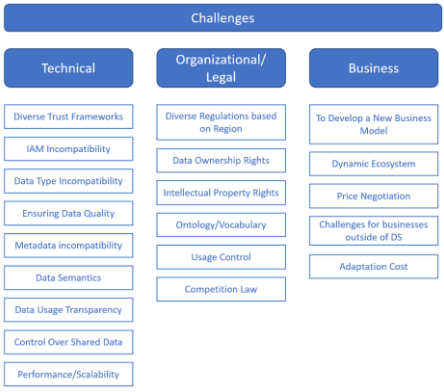

Figure 2 Challenges in Data Exchange

Personal data: Person dataspace is one of the most challenging, considering its criticality. In the EU, eIDAS 2.0 is one of the main trust frameworks for organisations, regardless of whether they are governmental or non-governmental, to deal with data in a secure way. It aims to give individuals control over their data, and in this way, it is possible to avoid massive personal data breaches or honeypots. However, the suggested paradigm is incomplete and contains security flaws. The aforementioned points are supported by the German IDWallet incidents, in which sensitive personal data was released to unaffiliated parties without the required authentication [SDI22].

Finance: The challenges that financial data interchange must overcome are numerous and need careful planning. Considering that financial data is one of the most powerful data that gives a lot of information about individuals, it requires strong encryption, authentication, and consent management are essential to guaranteeing data privacy and security. Interoperability, consistency, and data validation are common needs shared by various industries. Dealing with the date and time is very important, especially when there is cross-border data interchange where is requires specific adjustment to the

established ecosystem.

4 Conclusion

Data is a valuable asset, thus gathering more of it will increase its value. On the other hand, data in silos cannot be used to its full potential, so data exchange is a requirement. A trusted environment that facilitates seamless transactions is necessary for the data exchange process. In the EU, data protection is given top attention, and numerous laws, rules, and data acts are in place. The drive for greater cooperation is hampered by how difficult it is to follow each guideline precisely for each partnership. In order to ease this process dataspace gives stakeholders high interoperability while enabling data exchange in a safe and trustworthy environment. Gaia-X provides a framework to follow these sets of rules and regulations while starting a Dataspace. Gaia-X regulations are very well aligned with EU data and cloud strategies which means all the regulations are taken into account. As providing regulation frameworks is not enough for building a Dataspace, IDS-RAM proposed a blueprint architecture for data exchange. Gaia-X and IDSA architectures led several organisations to launch dataspace projects in various industries including German Mobility Dataspace, Catena-X, MyData Global and others that have been covered in this paper. This paper provided a thorough analysis of the trust establishment in data exchange, including reference architectures, adaptable areas, involved organisations, and state-of-the-art. However, because the data providers come from a variety of backgrounds, including technical and legal differences, it is highly challenging to develop perfect interoperability together with high security.

Bibliography

[ID24] International Data Space Association. International Data Spaces. URL: https://internationaldataspaces.org/ (acc. 02/01/2024)

[Ga24] Gaia-X. Gaia-X. URL: https://gaia-x.eu/ (acc. 02/01/2024).

[Je22] Jeyakumar, J., et al. "A novel approach to establish trust in verifiable credential issuers in Self-sovereign identity ecosystems using TRAIN." In Open Identity Summit 2022, 2022.

[La23] Larsen, B., et al. "Achieving Higher Level of Assurance in Privacy Preserving Identity Wallets." URL: www.ioanniskrontiris.de/publications/2023937.pdf (acc. 02/01/2024).

[CFH22] Plappert, C., Andreas, F., & Ronald H. "Analysis and Evaluation of Hardware Trust Anchors in the Automotive Domain." In Proceedings of the 17th International Conference on Availability, Reliability and Security, 2022.

[EM24] Alalwany, E., Imad, M. "Security and Trust Management in the Internet of Vehicles (IoV): Challenges and Machine Learning Solutions." Sensors 24.2 (2024): 368.

[Ku23] Kubach, M., et al. "A shared responsibility model to support cross border and cross organizational federation on top of decentralized and self-sovereign identity: Architecture and first PoC." In Open Identity Summit 2023, 2023.

[Sa16] Sambra, A.V., et al. "Solid: a platform for decentralized social applications based on linked data." MIT CSAIL & Qatar Computing Research Institute, Tech. Rep., 2016.

[Co24] Collaborative and Confidential Information Sharing. URL: https://c3isp.eu/ (acc. 02/01/2024).

[Ed24] Edge enabled Privacy and Security Platform for Multi Modal Transport. URL: https://e-corridor.eu/ (acc. 02/01/2024).

[Ch23] Chen, Z., et al. "OPAL: Ontology-Aware Pretrained Language Model for End-to-End Task-Oriented Dialogue." Transactions of the Association for Computational Linguistics 11 (2023): 68-84.

[Da19] Davie, M., et al. "The trust over ip stack." IEEE Communications Standards Magazine 3.4 (2019): 46-51.

[DS24] Data Spaces Business Alliance. Data Spaces Business Alliance. URL: https://data-spaces-business-alliance.eu/ (acc. 02/01/2024).

[Ei24] eIDAS Regulation. URL: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation (acc. 02/01/2024).

[Ca24] Catena-X. Catena-X. URL: https://catena-x.net/en/ (acc. 02/01/2024).

[GM24] German Mobility Dataspace. URL: https://mobility-dataspace.eu/ (acc. 02/01/2024).

[Ma24] Manufacturing-X. Manufacturing-X. URL: https://www.plattform-i40.de/IP/Navigation/EN/Manufacturing-X/Manufacturing-X.html (acc. 02/01/2024).

[My24] My Data Global. My Data Global. URL: https://mydata.org/ (acc. 02/01/2024).

[En24] aNewGovernance. aNewGovernance. URL: https://www.anewgovernance.org/(acc. 02/01/2024).

[Da24] Data Space for Skills. Data Space for Skills. URL: https://www.skillsdataspace.eu/(acc. 02/01/2024).

[Pr24] Prometheus-x. Prometheus-x. URL: https://prometheus-x.org/?locale=en(acc. 02/01/2024).

[Ma23] Marelli, L., et al. "The European Health Data Space: Too Big To Succeed?." Health Policy (2023): 104861.

[SAA22] Schwalm, S., Daria, A., & Ignacio, A. "eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI." In Open Identity Summit 2022, 2022.

[SLW21] Stalla-Bourdillon, S., Laura, C., & Alexsis, W. "Fostering trustworthy data sharing: Establishing data foundations in practice." Data & Policy 3 (2021).