Exploiting Data Spaces to Enable Privacy Preserving Data Exchange in the Energy Supply Chain

Luigi Coppolino[1,*], Alessandro De Crecchio[2,*], Roberto Nardone[2,*], Alfredo Petruolo[1,*], Luigi Romano[1,*] and Federica Uccello[1]

[1]University of Naples 'Parthenope', Centro Direzionale, 80143 Naples, Italy
[2]Scuola IMT Alti Studi Lucca, Piazza S. Ponziano, Lucca

Abstract

In the modern digital landscape, ensuring secure data sharing within complex infrastructures is not trivial. This paper presents an in-depth analysis of dataspaces and their crucial role in enhancing privacy-preserving data exchange within the energy supply chain. The main contribution of the work includes the design of the architecture of dataspaces, emphasizing their utility in addressing legal and technical challenges while ensuring data sovereignty and stakeholder trust. Through a focused case study and STRIDE analysis, the practical application and security benefits of dataspaces are illustrated, underscoring their significance in fostering a secure, efficient, and collaborative data-sharing environment.

Keywords

Smart Grid, Cybersecurity, Cyber Attack, FIWARE

1. Introduction

In today's interconnected world, existing systems are asked to fulfil increasing data-sharing requirements. The rapid expansion of data-centric applications underscoring the real value of data [1, 2] also affected smart grids and the energy supply chains. With a specific focus on energy exchange, current data exchange methods exhibit limitations, particularly when multiple stakeholders, including Transmission System Operators (TSOs) and Distribution System Operators (DSOs), need to collaborate and share sensitive information. The evolution introduced by the 'Common European Dataspaces' represents a strategic response to these challenges, fostering an environment where data can be exchanged securely and efficiently while respecting privacy and data sovereignty [3, 4].

While the importance of a unified data-sharing ecosystem is evident, the energy sector faces specific privacy and security challenges that need to be addressed. As an example, the integration and exchange of data among energy stakeholders necessitates robust privacy-preserving mechanisms to prevent unauthorized access and to ensure the integrity and confidentiality of the exchanged information. This is crucial for maintaining operational security and trust within

ITASEC 2024: The Italian Conference on CyberSecurity
*Corresponding author.
luigi.coppolino@uniparthenope.it (L. Coppolino); alessandro.decrecchio@imtlucca.it (A. De Crecchio); roberto.nardone@uniparthenope.it (R. Nardone); alfredo.petruolo001@studenti.uniparthenope.it (A. Petruolo); luigi.romano@uniparthenope.it (L. Romano); federica.uccello@assegnista.uniparthenope.it (F. Uccello)
0000-0002-2079-8713 (L. Coppolino); 0009-0003-6257-9732 (A. De Crecchio); 0000-0003-4938-9216 (R. Nardone); 0009-0003-2970-5864 (A. Petruolo); 0000-0003-2571-8572 (L. Romano); 0000-0001-9243-7047 (F. Uccello)

and across the energy supply chain [5]. Hence, prioritizing privacy-preserving data exchange and ensuring data sovereignty are basic requirements guiding this transformation [6].

The remainder of this paper is structured as follows. Section 2 addresses the related work. Section 3 offers a comprehensive overview to clarify the concept of dataspace and to address the ambiguities and uncertainties identified. Section 4 outlines specific European initiatives promoting the advancement of dataspaces, while Section 5 concentrates on efforts pertinent to the development and enhancement of dataspaces supporting the energy supply chain. Section 6 explores a practical case study where the dataspace paradigm has been applied, providing an analysis of security considerations and employing STRIDE methodology to assess communications based on dataspaces. Lastly, Section 7 ends the paper drawing final remarks.

2. Related Work

The challenges linked to privacy-preserving and secure data sharing have been subject to multiple research works. Among others, blockchain-based solutions have been proposed in several application domains [7, 8, 9, 10], exploiting the inherent properties of such technology to ensure traceability and integrity. Some others consider security and privacy, mainly using encryption algorithms. The work in [11] proposes a framework for sharing encrypted data in the cloud, addressing concerns about privacy breaches. A different approach is in [12], where two data-sharing algorithms are designed and evaluated in the context of Industrial IoT. Different frameworks with a specific focus on data sharing and standardized data formats have been proposed in different works, as [13, 14, 15, 16]. These frameworks adopt centralized data management, where data are acquired and then processed more than shared.

The present research is motivated by the specific need for privacy-preserving data exchange in the energy supply chain, aiming to clarify and tailor the concept of data spaces to this context. Additionally, advanced privacy-preserving techniques suited for the energy sector's demand are identified and deployed. Furthermore, a detailed case study is presented, applying STRIDE analysis to develop a targeted threat model for data exchange among energy stakeholders. The scope of the model is to demonstrate how dataspaces can enhance data security and privacy in the energy supply chain, aligning with European data strategy goals and fortifying resilience against cyber threats.

3. Data Spaces and Data Sovereignty in Europe

To the best of the authors' understanding, identifying a universally acknowledged definition of "dataspace" appears unfeasible. The GAIA-X initiative provides an initial perspective, describing dataspaces as federated, open infrastructures that facilitate data sharing and sovereignty, based on unified policies, rules, and standards [17]. Similarly, Open DEI defines dataspaces as decentralized infrastructures that ensure trustworthy data sharing and exchange within data ecosystems, adhering to mutually accepted principles [18]. Meanwhile, the European Commission envisions a dataspace as a unified global marketplace for both personal and non-personal data, including sensitive business information, and ensuring robust safeguards while providing businesses with easy access to top-quality industrial data to drive growth and innovation[19].

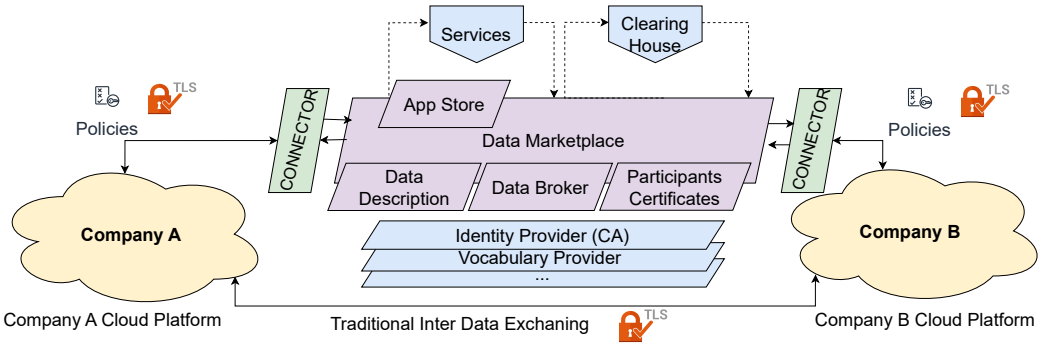

Figure 1: Dataspace-Based Data Exchaning

Given these different definitions and the consequent complexity of such a concept, this section aims to offer a concise yet right-to-the-point description of a dataspace, detailing the essential requirements and elucidating the key roles of privacy-preserving mechanisms and data sovereignty in its definition.

What a Dataspace Is. A dataspace is an open ecosystem facilitating data sharing and accessibility among different entities. This shift towards dataspaces relies on principles of transparency and trust that govern these ecosystems. Traditional data exchange methods face numerous challenges: a primary concern dataspaces seek to mitigate is the complexities stakeholders experience when establishing legal frameworks for collaboration. Stakeholders across vital sectors, like energy, encounter obstacles in creating contracts and establishing reliable data-sharing policies, hindering broader participation and innovation due to legal complexities. Conventional data exchange lacks full control over post-exchange data, posing risks in scenarios where data governance is crucial, potentially resulting in financial losses.

What a Dataspace Requires. To establish a collaborative and open environment for data sharing, developing a trusted ecosystem where each participant is recognized, has assigned roles, and is authorized for dataspace activities, is essential. Techniques ensuring privacy-preserving data exchange, authentication, authorization, and overall security are vital, as highlighted in the European Claim for dataspaces [20]. For this reason, dataspaces are designed to ensure data sovereignty, providing a framework where data owners maintain control over the usage and sharing of their data. This is a key concept in establishing trust and encouraging more entities to participate in data sharing, as it ensures the respect of their data rights and privacy. In a dataspace, ensuring compliance with regulations and ethical standards is vital, alongside an interoperable infrastructure supporting data sharing across diverse systems, achieved through common standards, vocabulary, and protocols.

Privacy-Preserving Data Exchange. In the dataspace paradigm, data exchange is enabled through connectors, which can be deployed on-premises or in a cloud environment, primarily using helm charts and Kubernetes clusters, following an architecture ensuring security mechanisms. As depicted in Figure 1, establishing the data marketplace requires, among others, a Certification Authority (CA) and a shared vocabulary. The former ensures that different stakeholders can be identified and authorized to participate in the marketplace, while the latter

enables participants to comprehend a shared language. This common understanding is essential for facilitating machine-to-machine (M2M) communication and simplifying the creation of privacy-preserving policies. From a technical perspective, it is also essential to guarantee the minimum requirements needed for stakeholders' computing nodes, verify the level of security provided (e.g., Trusted Execution Environment support [21]), and confirm their geographical locations. Stakeholders can publish descriptions of their data offerings on a data broker, while developers can provide applications that utilize this data to create added-value services. All transactions between different connectors are recorded by a clearing house, to ensure the accurate processing of payments and data exchanges. Examples of policy enforcement in dataspaces include restrictions on the duration of data usage, the rights to view and utilize data, and the conditions under which data may be shared or processed. For instance, policies might dictate that certain data can only be accessed for a limited time, or specify that data must not be transferred to unauthorized parties. Additionally, policies can enforce data anonymization or de-identification before it is shared to protect privacy. These rules ensure that all data handling within the dataspace adheres to agreed-upon ethical and legal standards, fostering a secure and trusted environment for all participants.

4. The European Initiatives for Data Spaces

The evolving data-driven landscape and the need for value-added services drive European efforts to establish Common European data spaces [22]. This section highlights the key stakeholders shaping this shift to a novel paradigm, prioritizing European values and facilitating new criteria for data sharing.

4.1. International Data Space Association

The International Data Space Association [23] (IDSA) plays a significant role in the data-sharing revolution. Its mission focuses on ensuring data sovereignty and bridging the gap between industry and research communities to establish data spaces. From a technical point of view, the association has devised the IDSA RAM [24], a reference architecture that delineates the technical and organizational principles for implementing dataspaces. The Reference Model (Figure 2) encompasses three primary aspects: security, certificates, and governance, organized into five layers of granularity: Business, Functional, Information, Process, and System. The Business Layer is devoted to articulating business models and value chains, clarifying the roles and interactions of stakeholders to ensure alignment with business goals. In the Functional Layer, the key capabilities and services necessary for data exchange are delineated, including specific functions such as data sharing and processing that underpin business requirements. The focus of the Information Layer is on organizing data, defining its semantics, and managing its governance to guarantee that data can be exchanged and interpreted across diverse systems. The Process Layer concentrates on the operational aspects, defining the processes and protocols that ensure data is exchanged securely and efficiently, adhering to established policies and standards. Lastly, the System Layer is concerned with the technical foundation, specifying the necessary infrastructure and components, like connectors and networks, that enable the secure exchange of data within the data space. IDSA's key contribution includes the specification of

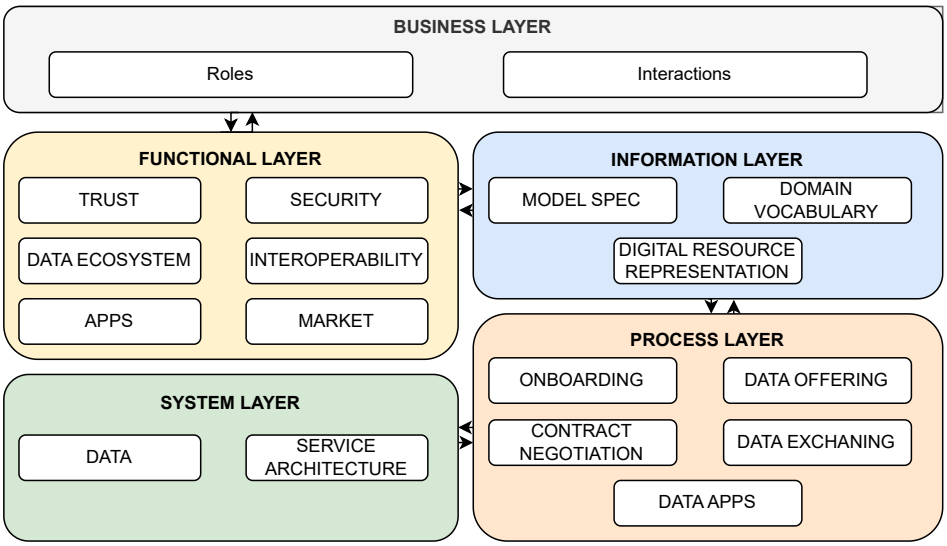

Figure 2: IDSA RAM Architecture Specification.

Connectors, essential for establishing a dataspace instance. These, detailed in the IDSA RAM, enable multiple parties to create the data-sharing platform.

4.2. FIWARE

As data-driven technologies are becoming increasingly integral in today's digital world [25], the FIWARE foundation plays a crucial role in supporting the development of smart applications and services [26, 27]. FIWARE provides open-source software enabling developers to craft data-centric applications. The building blocks are the Generic Enablers, which offer a range of functionalities to integrate various data sources and services. This enhanced ecosystem of open-source resources is crafted to optimize the development process, simplifying and accelerating the ability of developers to create advanced, data-centric solutions. FIWARE is crucial in the realization of Digital Twins: the core is the Context Broker, a Generic Enabler that orchestrates the management and storage of context information, bridging the physical devices and their digital replicas. The Context Broker acts as a central hub, ensuring consistent, up-to-date context information between various data sources and applications. It synchronizes real-world entities with digital twin models, enabling real-time responsiveness and dynamic updates. FIWARE's commitment to interoperability and manufacturer-independent solutions is evident in its IoT agents, which translate messages from diverse protocols into a standardized format, facilitating the creation of manufacturer-agnostic solutions within the FIWARE ecosystem.

This approach is fundamental in advancing the concept of data spaces, where diverse data sources and systems coalesce in a unified, interoperable environment. Additionally, FIWARE's contribution extends to the standardization of data models through its Smart Data Models initiative. This effort provides a common vocabulary and a set of standardized data structures, vital for the homogenization of data and the facilitation of interoperable data exchange. These

data models offer significant value in the context of data spaces, enabling disparate systems to understand and interpret shared data consistently, and enhancing collaboration and innovation in data-driven environments.

5. The Energy Data Space and the CIM

The European Common Data Spaces in the energy sector are crucial for several reasons as illustrated in Table 1. It offers key benefits and enables utilities and governments to develop new services for citizens and uncover new revenue streams. It is a transformative paradigm in the energy sector, uniting stakeholders—energy providers, consumers, grid operators, and regulators—under a shared digital context. This unification is not only about connecting dots but about creating a secure exchange of data that bridges the traditional silos, fostering a seamless flow of information and insights across the energy landscape. Such integration and interoperability are fundamental for the sector's efficient resource management and distribution, ensuring that energy reaches where it is needed most when it is needed. Within this context, initiatives like Enershare [28] and CyberSEAS [29] emerge in the realization of this vision. Enershare's objectives are emblematic of the broader ambitions of the European Common Data Spaces. It aims to democratize energy data, making it accessible and actionable for a spectrum of stakeholders. This democratization is not only about data sharing but about creating a platform where this data can be transformed into actionable intelligence, driving decision-making, and innovation across the energy sector. In Particular, Enershare focuses on harnessing the power of shared data to enable more sustainable energy practices, enhance grid efficiency, and foster the development of new business models and services that can contribute to the energy transition. Indeed, the CyberSEAS Project, funded by the EU, targets the crucial objective of securing European data spaces among its strategic objectives. This initiative underscores the importance of robust security measures in the realm of data sharing and exchange. CyberSEAS is dedicated to advancing applications of enabling technologies that are crucial for facilitating privacy-preserving data exchange and sharing among various utility operators. By focusing on these technologies, the project aims to establish a secure framework that ensures data confidentiality and integrity across different entities within the utility sector, enhancing trust and collaboration in European data spaces.

The significance of establishing data exchange mechanisms among various operators and stakeholders within the energy supply chain is well acknowledged. This aspect has been addressed in the energy domain through the adoption of standardized schemas for representing assets. This has been made possible by the existence of an industry standard, the IEC 61970 Series, commonly referred to as the Common Information Model (CIM) [34]. The CIM fosters interoperability, enabling seamless integration and communication across different systems and platforms used by utility operators and stakeholders. By adhering to CIM standards, organizations can achieve consistency in data representation, ensuring that critical information about assets, operations, and grid conditions is accurately interpreted and shared among relevant parties. CIM is implemented using RDF (Resource Description Framework). In this context, RDF is used to define the hierarchical structure of CIM classes and their relationships. Each CIM class, such as Substation or VoltageLevel, is represented as a resource identified by a unique

Benefit	Description
Optimized Energy Distribution	Enables more efficient management and distribution of energy resources by leveraging data on consumption, production, and grid status [30].
Enhanced Energy Efficiency	Facilitates better understanding and management of energy consumption, promoting energy-saving measures and technologies [31].
Monitoring Facilitation	Supports the integration and effective monitoring of energy assets within the energy grid [32].
Innovative Services Development	Empowers the creation of new, data-driven services for consumers, enhancing user experience and engagement [33].

Table 1
Key Benefits of Data Spaces in the Energy Sector

URI (Uniform Resource Identifier). Predicates encapsulate the properties and attributes of CIM classes, while their respective values are embodied as objects. CIM schemas enable Transmission System Operators (TSOs) to readily access real-time information on RES generation output, thereby empowering them to effectively balance supply and demand. Likewise, Distribution System Operators (DSOs) leverage CIM to acquire data on distributed energy resources (DERs), which supports grid planning and operation. Therefore, when developing an energy data space, ensuring services compliant with this schema representation should not be overlooked. To effectively harness the benefits of CIM while mitigating its drawbacks, the solution is the development of dataspace services and data applications that are compliant with CIM standards.

6. A Case Study: Cross-Border Energy Data Sharing

This section describes a case study focused on the sharing of energy data, which shows how the strategic alignment of diverse stakeholder requirements can benefit from a more unified and effective power grid management. It demonstrates that substantial benefits derive from advanced data-sharing mechanisms within a well-structured dataspace. This case study comes from the experience with utility operators, within the CyberSEAS project [29], from multiple national stakeholders involving a wide array of end-users, integrating them into the dataspace to enhance collective outcomes. The final objective is to create an environment where stakeholders can exchange vital infrastructure data, thereby enriching the ecosystem's value and functionality. This approach also played a pivotal role in providing essential protections for the public, mitigating cybersecurity risks that could influence critical services, including billing. The case study allows us to point out the twofold benefit of the proposed approach: augmenting operational efficiency and fulfilling the consumers' privacy.

6.1. Data Flow Diagram and Threat Model

As anticipated in Section 5, to secure the common European energy data space we follow the STRIDE methodology in conjunction with Data Flow Diagrams (DFDs). The initial phase

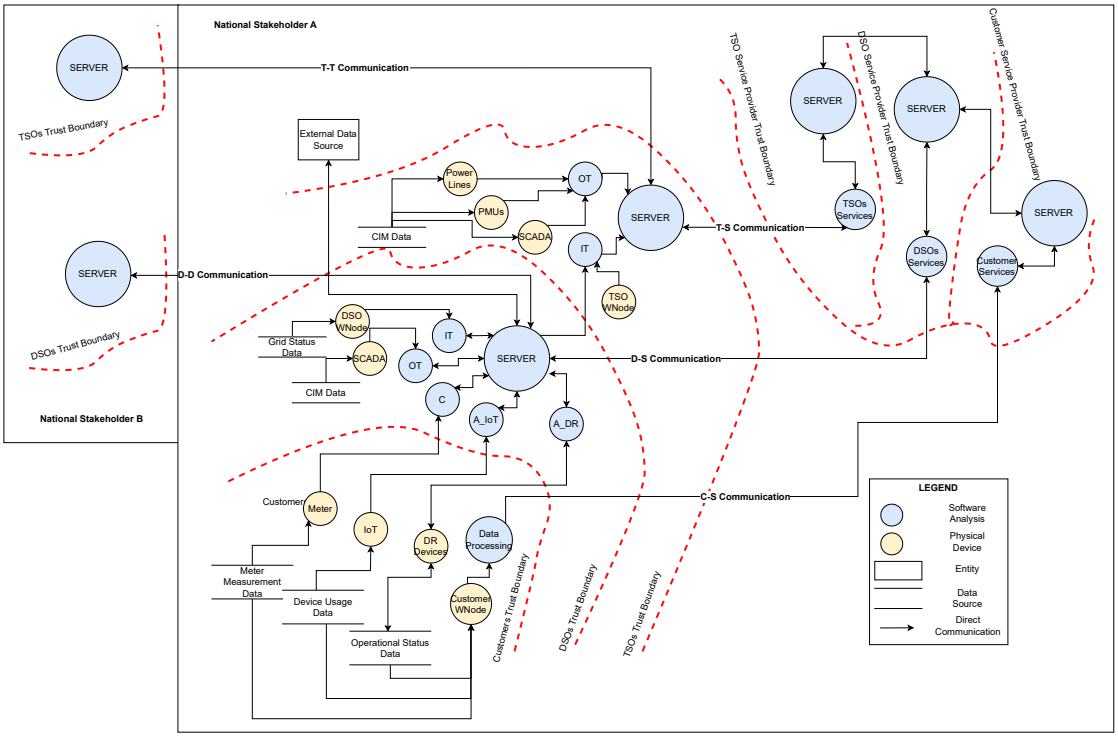

Figure 3: Energy Stakeholders Data Flow Diagram

applies the STRIDE threat modelling framework and involves the identification of the system's boundaries and the construction of the DFD, shown in Figure 3. This diagram identifies different trust boundaries for each participant in the energy dataspace, acknowledging the premise that different entities do not inherently trust one another. The diagram reports the various energy sector stakeholders, such as TSOs and DSOs, abstracting their complex internal communications. In particular, this DFD shows how data related to the power grid's operational status and the CIM infrastructural descriptions are essential for the operational and strategic management of the grid. These data aspects are crucial for TSOs and DSOs to access real-time information and for supporting grid planning and operational decisions. Another delineated trust boundary pertains to customer premises. Data from meters, IoT devices, and Demand Response assets (DR Devices) can be collected by the utility operator or leveraged to develop new services to enhance power savings, among other objectives. Beyond direct communication with the utility provider, there may also be data exchanges with untrusted parties, such as cloud-based IoT control mechanisms that could be hosted globally. This potential interaction warrants careful consideration within the threat modelling effort.

Once we have delineated the entire system, we map the assets identified in the DFD with their corresponding STRIDE threats. This mapping enables us to associate each asset with the specific security threats it may face, providing a comprehensive understanding of the potential risks within the system. As depicted in Table 2, each device within this system is subject to various threats that must be carefully considered. When analyzing the dataspace-facilitated interactions,

it is crucial to recognize that privacy-preserving techniques and policy enforcement measures must be specifically tailored to address these threats. For example, strong authentication mechanisms such as multi-factor authentication can be implemented to counteract spoofing. Policy enforcement can be strengthened by using attribute-based access controls (ABAC) to fine-tune who has access to data under what conditions. Furthermore, to protect against information disclosure, data can be encrypted both at rest and in transit, ensuring that sensitive information remains confidential. These measures, when carefully specified and applied, can significantly bolster the security of dataspace interactions.

6.2. Dataspace-based solution

While the establishment of dataspace-based communication enables participants to devise their policies for ensuring privacy during data exchanges, it's important to highlight the intricate complexities involved in this solution. Specifically, the adoption of a common vocabulary has been facilitated through the use of smart data models from FIWARE, particularly those related to the Common Information Model (CIM). This adoption has streamlined the implementation of communication, allowing participants to comprehend a shared language and exchange valuable data effectively for information creation. However, another potential drawback is the reliance on such standardized models, which may not always accommodate the specific needs or nuances of all participating entities. While standardization promotes interoperability and simplifies data sharing, it can also constrain organizations' flexibility to represent their data in ways that fully capture its unique aspects or proprietary nuances. Additionally, aligning different data models to a common standard can be resource-intensive and require significant transformation or mapping efforts, which could introduce data fidelity concerns. The resulting framework is depicted in Figure 4, where the interactions among different national stakeholders (including TSOs and DSOs) and (potential) service providers through the dataspace are mediated by a set of security policies, well-defined and enforced by the cited technologies and frameworks. It is important to acknowledge that this set of policies has to be dynamically updated and adjusted when it is needed.

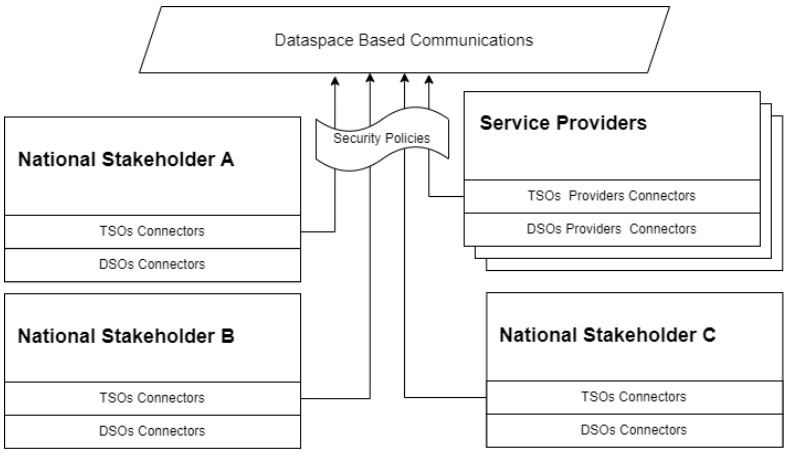

Figure 4: Dataspace-based solution.

Asset	Description	STRIDE Element
TSO/DSO Systems	Entities managing the transmission and distribution of energy	Spoofing, Tampering, Repudiation
SCADA Systems	Systems for monitoring and controlling industrial processes	Information Disclosure, Denial of Service
Operational Technology	Hardware and software that monitors and controls physical devices	Elevation of Privilege, Tampering
Information Technology	Systems used for managing and processing information	Spoofing, Information Disclosure, Denial of Service
Smart Meters	Devices that measure energy usage and communicate this information	Information Disclosure, Denial of Service
IoT Devices	Devices connected to the internet that collect and exchange data	Elevation of Privilege, Information Disclosure, Denial of Service
Demand Response Devices	Devices that manage energy usage based on demand signals	Denial of Service, Tampering
Working Nodes (WNode)	Nodes responsible for data transmission within the network	Denial of Service, Spoofing, Information Disclosure
Common Information Model (CIM) Data Sources	Standardized models describing electrical components and configurations	Tampering, Information Disclosure, Denial of Service
Grid Status Data Sources	Systems providing real-time data on the status of the electrical grid	Tampering, Information Disclosure
External Data Sources	External systems providing additional data, like weather services	Spoofing, Information Disclosure
Concentrators Analysis	Analysis of the data collected from smart meters	Spoofing, Tampering, Information Disclosure
IoT Aggregator Analysis	Systems that compile and manage data from multiple IoT devices	Spoofing, Elevation of Privilege, Information Disclosure
Demand Response Aggregator Analysis	Systems that manage and coordinate demand response signals and data	Spoofing, Tampering, Denial of Service

Table 2
Assets and Corresponding STRIDE Elements in the Energy Dataspace

Example of Policy Enforcement Loop for Securing Connectors. A dynamic approach to enforce security policies in dataspace connectors begins with the initialization of the connector using baseline security policies and the importation of an initial STRIDE-based threat model. The enforcement process is structured as a continuous loop that only concludes when the connector is deactivated. Within this loop, the connector first collects real-time data on its interactions. Simultaneously, it integrates both external threat intelligence and insights from

internal monitoring logs to comprehensively update the threat model. As the loop continues, for each type of interaction that the connector facilitates, it is important to assess whether the existing security policies adequately mitigate the identified risks. This approach involves strengthening authentication protocols, refining access controls, and bolstering data encryption to counteract the assessed threats. Finally after implementing the necessary adjustments, these updated policies are enforced in real time. This proactive and adaptive approach ensures the connectors are secured against evolving threats throughout their operational life.

7. Summary and Conclusions

This paper focuses on the pressing need for methods of exchanging data that preserve privacy and has shed light on the emerging paradigm of dataspaces. These innovative ecosystems allow for the free flow of data among various parties, facilitating the establishment of domain-specific data markets that offer novel solutions for stakeholders in industry, research, and institutions. Among the primary contributions, the work addressed the definition, requirements, and privacy-preserving techniques of the dataspace. Then, the most significant European initiatives focusing on dataspaces utilization and contribution to security were presented. Finally, a real-world case study was shown, to demonstrate the practical applications, the potential benefits, and the challenges associated with the adoption of this paradigm. The present research highlights the significant opportunities offered by data sovereignty in improving data exchange across various sectors. However, realizing its full potential requires a thorough understanding of its operational dynamics and security measures, to ensure stakeholders fully comprehend its benefits. By promoting understanding and facilitating the adoption of this paradigm, steps forward can be made toward secure and efficient data exchange, with a focus on individual and organizational data rights.

Acknowledgments

This research has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560 CyberSEAS. The content of this publication reflects the opinion of its authors and does not, in any way, represent the opinions of the European Union. The European Commission is not responsible for any use that may be made of the information that this publication contains.

This work has been also partially funded by the European Union under NextGenerationEU PRIN 2022 Prot. n. 202297YF75 S2: Safe and Secure Industrial Internet of Things. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.

References

[1] C. Acciarini, F. Cappa, P. Boccardelli, R. Oriani, How can organizations leverage big data to innovate their business models? A systematic literature review, Technovation 123 (2023)

102713.
[2] S. Bose, S. K. Dey, S. Bhattacharjee, Big data, data analytics and artificial intelligence in accounting: An overview, Handbook of Big Data Research Methods: 0 (2023) 32.
[3] B. Otto, A federated infrastructure for european data spaces, Communications of the ACM 65 (2022) 44–45.
[4] B. Otto, M. ten Hompel, S. Wrobel, Designing Data Spaces: The Ecosystem Approach to Competitive Advantage, Springer Nature, 2022.
[5] M. Huber, S. Wessel, G. Brost, N. Menz, Building trust in data spaces, Designing Data Spaces (2022) 147.
[6] P. Hummel, M. Braun, M. Tretter, P. Dabrock, Data sovereignty: A review, Big Data & Society 8 (2021) 2053951720982012.
[7] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, W. Ni, Privysharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities, Computers & Security 88 (2020) 101653.
[8] B. Le Nguyen, E. L. Lydia, M. Elhoseny, I. Pustokhina, D. A. Pustokhin, M. M. Selim, G. N. Nguyen, K. Shankar, Privacy preserving blockchain technique to achieve secure and reliable sharing of iot data, Computers, Materials & Continua 65 (2020) 87–107.
[9] F. Buccafurri, V. De Angelis, M. F. Idone, C. Labrini, A protocol for anonymous short communications in social networks and its application to proximity-based services, Online Social Networks and Media 31 (2022) 100221. URL: https://www.sciencedirect.com/science/article/pii/S2468696422000258. doi:https://doi.org/10.1016/j.osnem.2022.100221.
[10] L. Tan, K. Yu, N. Shi, C. Yang, W. Wei, H. Lu, Towards secure and privacy-preserving data sharing for covid-19 medical records: A blockchain-empowered approach, IEEE Transactions on Network Science and Engineering 9 (2021) 271–281.
[11] J. Sun, G. Xu, T. Zhang, H. Xiong, H. Li, R. H. Deng, Share your data carefree: An efficient, scalable and privacy-preserving data sharing service in cloud computing, IEEE Transactions on Cloud Computing 11 (2021) 822–838.
[12] X. Zheng, Z. Cai, Privacy-preserved data sharing towards multiple parties in industrial iots, IEEE Journal on Selected Areas in Communications 38 (2020) 968–979.
[13] L. Coppolino, S. D'Antonio, R. Nardone, L. Romano, A self-adaptation-based approach to resilience improvement of complex internets of utility systems, Environment Systems and Decisions 43 (2023) 708–720.
[14] F. Buccafurri, V. de Angelis, S. Lazzaro, Mqtt-a: A broker-bridging p2p architecture to achieve anonymity in mqtt, IEEE Internet of Things Journal 10 (2023) 15443–15463. doi:10.1109/JIOT.2023.3264019.
[15] L. Coppolino, S. D'Antonio, G. Mazzeo, L. Romano, L. Sgaglione, Prisiem: Enabling privacy-preserving managed security services, Journal of network and computer applications 203 (2022) 103397.
[16] L. Coppolino, S. D'Antonio, V. Giuliano, G. Mazzeo, L. Romano, A framework for seveso-compliant cyber-physical security testing in sensitive industrial plants, Computers in Industry 136 (2022) 103589.
[17] Gaia-X Hub, White paper: What is a data space?, 2022. URL: https://gaia-x-hub.de/wp-content/uploads/2022/10/White_Paper_Definition_Dataspace_EN.pdf, accessed: 2024-02-26.

[18] Open DEI, Position paper: Design principles for data spaces, 2022. URL: https://www.opendei.eu/wp-content/uploads/2022/03/Position-Paper-Design-Principles-for-Data-Spaces.pdf, accessed: 2024-02-26.
[19] European Commission, European Data Spaces, Technical Report, Publications Office of the European Union, 2023. URL: https://op.europa.eu/en/publication-detail/-/publication/dcac6aee-0e7a-11ee-b12e-01aa75ed71a1/language-en, accessed: 2024-02-26.
[20] European Commission, Data Spaces, 2024. URL: https://digital-strategy.ec.europa.eu/en/policies/data-spaces, accessed: 2024-02-26.
[21] L. Coppolino, R. Nardone, A. Petruolo, L. Romano, Securing fiware with tee technology, in: New Trends in Intelligent Software Methodologies, Tools and Techniques: Proceedings of the 22nd International Conference on New Trends in Intelligent Software Methodologies, Tools and Techniques (SoMeT_23), volume 371, IOS Press, 2023, p. 149.
[22] E. Union, Commission staff working document on common european data spaces, 2020. URL: https://op.europa.eu/en/publication-detail/-/publication/dcac6aee-0e7a-11ee-b12e-01aa75ed71a1/language-en, retrieved from https://op.europa.eu/.
[23] International Data Spaces, 2024. URL: https://internationaldataspaces.org/.
[24] I. D. S. Association, International data spaces reference architecture model (ids-ram) 4.0, 2023. URL: https://github.com/International-Data-Spaces-Association/IDS-RAM_4_0.
[25] M. A. Camilleri, The use of data-driven technologies for customer-centric marketing, International Journal of Big Data Management 1 (2020) 50–63.
[26] Á. Alonso, A. Pozo, J. M. Cantera, F. De la Vega, J. J. Hierro, Industrial data space architecture implementation using fiware, Sensors 18 (2018) 2226.
[27] L. Coppolino, R. Nardone, A. Petruolo, L. Romano, Building cyber-resilient smart grids with digital twins and data spaces, Applied Sciences 13 (2023) 13060.
[28] Enershare, Enershare | the energy data space for europe, 2024. URL: https://enershare.eu/.
[29] CyberSEAS | Cyber Securing Energy dAta Services, 2024. URL: https://cyberseas.eu/.
[30] V. Janev, M. E. Vidal, K. Endris, D. Pujic, Managing knowledge in energy data spaces, in: Companion Proceedings of the Web Conference 2021, 2021, pp. 7–15.
[31] E. Curry, S. Hasan, S. O'Riain, Enterprise energy management using a linked dataspace for energy intelligence, in: 2012 Sustainable Internet and ICT for Sustainability (SustainIT), 2012, pp. 1–6.
[32] L. Coppolino, R. Nardone, A. Petruolo, L. Romano, A. Souvent, Exploiting digital twin technology for cybersecurity monitoring in smart grids, in: Proceedings of the 18th International Conference on Availability, Reliability and Security, 2023, pp. 1–10.
[33] S. Meneguzzo, A. Favenza, V. Gatteschi, C. Schifanella, Integrating a dlt-based data marketplace with idsa for a unified energy dataspace: Towards silo-free energy data exchange within gaia-x, in: 2023 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), IEEE, 2023, pp. 1–2.
[34] M. Uslar, M. Specht, S. Rohjans, J. Trefke, J. M. González, The Common Information Model CIM: IEC 61968/61970 and 62325-A practical introduction to the CIM, Springer Science & Business Media, 2012.