IOTA-Enabled Decentralized Data Space for IIoT Ecosystems

Anhelina Kovach, Leticia Montalvillo, Aitor Urbieta
Ikerlan Technology Research Centre,
Basque Research and Technology Alliance (BRTA)
Arrasate-Mondragón, Spain
{akovach, lmontalvillo, aurbieta}@ikerlan.es

Jorge Lanza
Network Planning and Mobile Communications Lab,
University of Cantabria
Santander, Spain
jlanza@tlmat.unican.es

***Abstract*—Securing interoperable and sovereign data exchange in the Industrial Internet of Things (IIoT) for machine data exploitation by third parties presents a challenge. This work addresses this by integrating IOTA Distributed Ledger Technology (DLT) with the International Data Spaces (IDS) Reference Architecture Model (RAM), creating a decentralized data space optimized for IIoT ecosystems. Moving beyond traditional blockchains constrained by scalability and efficiency, our approach employs IOTA's Directed Acyclic Graph (DAG) for secure, scalable data storage and exchange. This research demonstrates the implementation of core IDS architectural concepts within the IOTA framework, advancing beyond theoretical DLT limitations and illustrating IOTA's ability to enhance data sovereignty and interoperability in the IIoT, setting the stage for future evaluations and broader applicability studies.**

***Index Terms*—Data Space, Distributed Ledger Technology, Eclipse Dataspace Components, International Data Spaces, IOTA, Self-Sovereign Identity, Verifiable Credentials**

Type of contribution: *Research in progress*

I. Introduction

The rise of Industry 4.0 and the proliferation of Industrial Internet of Things (IIoT) devices have redefined industrial ecosystems, placing data at the core of this new paradigm. The role of data in optimizing processes, enhancing production efficiency, and enabling precise operational monitoring is increasingly evident [1]. This paradigm highlights the need for systematic design and management of the entire data lifecycle, from the creation and collection of data, ensuring its integrity and provenance, to secure storage and efficient exploitation.

In the IIoT landscape, decentralized storage mechanisms provided by Distributed Ledger Technology (DLT) offer a robust approach to data management, enhancing security and immutability, crucial for data integrity and provenance [2]. The incorporation of Self-Sovereign Identity (SSI) enables identification within the industrial ecosystem, securing data storage and enabling precise traceability and provenance verification, thus improving data management across its lifecycle.

Building on the capabilities of IOTA's Tangle [3], a DLT that uses a Directed Acyclic Graph (DAG) structure, this article evaluates its potential as a robust foundation for IIoT applications [4], [5]. The IOTA architecture provides advantages for secure, scalable, and efficient data and value transfer in industrial environments. This research extends a platform previously described in [6], designed to facilitate a billing model for the use of rented industrial machinery between clients and suppliers, with transactions securely logged in the Tangle, building on the initial scenario depicted in Figure 1.

Acknowledging the evolving landscape of IIoT, this work aims to extend the platform's capabilities to enable the sharing and monetization of machine-generated data with third parties. The extension focuses on maintaining data sovereignty and secure usage within a broader ecosystem. This includes (*1*) enabling secure data exchange across multiple entities, (*2*) ensuring data sovereignty by enabling control over data access, usage, and compliance with regulatory requirements, (*3*) identifying and authenticating all ecosystem participants and components, (*4*) providing descriptive features, usage terms, and pricing for offered data assets, and (*5*) recording of all operations within the ecosystem.

This evolution necessitates adopting data space technology, an emerging solution that fosters secure data exchange under a common framework of trust and governance, facilitated by initiatives such as the International Data Spaces (IDS). This approach, which centers on establishing a shared technical infrastructure, addresses the requirement for secure, governed, and sovereign data exchange within a unified framework [7], a need not fully met by the IOTA framework. While IOTA ensures transaction security and data integrity, it needs more access control, governance, and interoperability across heterogeneous systems to ensure a common trust framework.

The primary focus of this work is to emphasize the practical application and benefits of integrating IDS within the IOTA ecosystem, enabling a use case for data exploitation. By implementing IDS Reference Architecture Model (RAM) [8] architectural concepts into IOTA's DLT and leveraging its frameworks, the integration aims to establish identity management, data cataloging, and logging functionalities, thus enhancing data sovereignty, sharing, governance, and interoperability. This detailed deployment and operation of the IOTA framework showcase its capacity to meet the demands of the data spaces domain. Furthermore, it elaborates on how these advancements pave the way for empirical evaluation and continuous improvement in industrial settings, ultimately facilitating data sharing across IIoT platforms.

This article is structured as follows: Section II introduces concepts such as DLT, SSI, and the data space paradigm, mainly focusing on the IDS architecture. Section III reviews related work and its limitations. Section IV elaborates on the processes to be implemented on the data space, while Section V introduces the proposed IOTA-enabled data space architecture. Section VI details the architecture's implementation and participant interactions. Section VII concludes by outlining future directions for this research in progress.

ISBN:978-84-09-62140-8

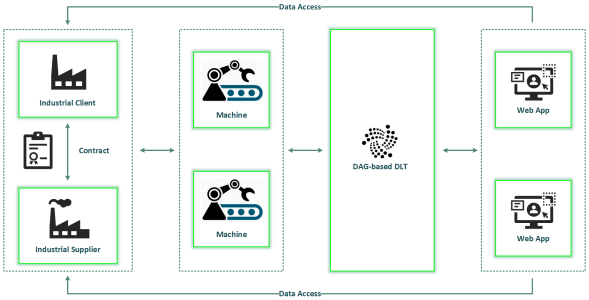

Figure 1: DLT data storage for machine usage billing

II. Background

This section provides an overview of distributed ledgers, particularly DAGs and its implementation on IOTA technology. It then briefly introduces SSI concepts and delves into the data spaces paradigm and the architecture proposed by the International Data Spaces Association (IDSA).

A. Distributed Ledger Technology

DLT encompasses distributed systems for data management, utilizing a network of nodes for decentralized control, thus enhancing transparency and consensus in data validation to identify malicious activities. In particular, blockchain and DAG-based networks are the two primary forms of DLT. Blockchain operates through a sequential chain of immutable transaction blocks, while DAG-based DLTs utilize directed graph structures to link transactions, enabling mutual validation. This approach improves scalability by facilitating the efficient processing of large volumes of transactions.

While blockchain faces scalability issues, transaction fees, and latency bottlenecks that degrade network performance [9], DAG technology overcomes these challenges. It provides a viable solution for high-throughput environments such as IIoT by eliminating transaction fees, enabling micro-transactions, and improving network agility and scalability through the multiple access points of its graph structure [10]. At a more practical level, IOTA's Tangle, a DAG-based DLT, not only overcomes blockchain's limitations but also provides a comprehensive ecosystem of solutions and frameworks for deploying additional services on its underlying network.

B. Self-Sovereign Identity

The SSI technology represents a significant advancement in data sovereignty, giving individuals complete control over their digital identities and challenging traditional intermediary-based identity management systems. This innovation allows users to control the specifics of data sharing, determining what data is shared, the terms of sharing, and the parties involved. At the core of SSI are digital identities and their associated Verifiable Credential (VC).

Digital identities, enabled by Decentralized Identifier (DID) [11], provide a decentralized and verifiable approach to digital identity, eliminating the need for centralized authorities [12]. A DID acts as a unique identifier pointing to a DID document containing verification methods, all stored on a secure ledger.

Complementing digital identities, VCs [13] attach attributes and claims to an identity authenticated by various verification methods. The SSI ecosystem includes key actors integrated into the narrative: (*1*) a Holder who owns VCs and can create a Verifiable Presentation (VP) for identity verification, (*2*) an Issuer who asserts claims on a subject and converts them into VCs for the holder, (*3*) a Verifier responsible for validating VPs against a data registry, and (*4*) a Verifiable Data Registry that maintains and verifies digital identities and their associated public keys, primarily through DLT.

C. Data Spaces

Data spaces are a distributed data integration concept where data providers deliver their data to consumers under a common technical and legislative standardized framework. Participants can contribute data while maintaining sovereignty over what data is shared, by whom, and for how long. This model ensures trust in data interactions and fosters an economic environment centered on data sharing while maintaining privacy and security [14].

On a legislative level, the European Union (EU) data spaces concept is driven by policies such as the European Strategy for Data [15], designed to enhance data access, sharing, and governance and aims at integrating sector-specific data spaces into a unified data market for the EU. This strategy is supported by the Open Data and Public Sector Information Directive [16], which promotes the re-use of public sector data, and Regulation (EU) 2018/1807 [17], ensuring the free flow of non-personal data within the EU. Together with the GDPR [18], which ensures data protection and privacy, the framework is further strengthened by the Data Governance Act [19] and the Data Act [20]. These legislative components collectively shape a robust legal framework that underpins the European Strategy for Data, guiding the development of various sector-specific data spaces and ensuring that data is accessible, secure, and governed by clear regulations.

The IDSA is an organization that brings together numerous industrial actors [21] to provide a technology-agnostic and standardized description of a data space distributed software architecture. It focuses on facilitating trustworthy data exchange between data providers and consumers, ensuring that all participants adhere to a common trust framework.

The IDS, developed and maintained by the IDSA, and Gaia-X are emerging as major initiatives in advancing data space frameworks rooted in the principles of data sovereignty and trust. While IDSA promotes a secure, decentralized framework for sharing data assets, Gaia-X is dedicated to building federated cloud services across multiple providers, promoting interoperability and mutual trust. Gaia-X differs from the more centralized, certificate-based X.509 approach described in the IDS RAM [8] by implementing a decentralized identity management system that leverages self-descriptions and VCs for services and participants [22].

A key enabler for participation in the data space is the connector [23], which ensures data sovereignty across the data lifecycle. Connectors go beyond facilitating data transfers as they offer functionalities for discovery, connection, contract negotiation, policy enforcement, and audit of transactions. They are embedded within the participants' infrastructure, enabling secure and compliant data communication.

IDS participants are classified into four categories concerning their role in the data space [24], as shown in Figure 2:

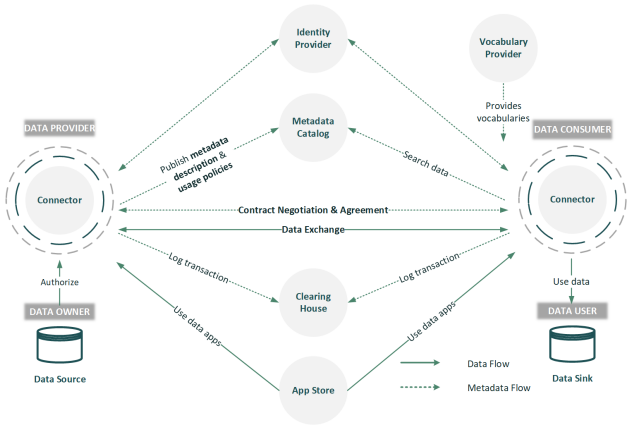

Figure 2: IDS architecture based on IDS RAM [8]

1) **Core Participants**: Entities involved and required every time data is exchanged.
   - Data Owner/Provider: Generates or owns data introduced into the IDS ecosystem. This implies the creation of data, establishing usage contracts, and setting policies to define how data can be accessed and used.
   - Data Consumer/User: Searches for data within the IDS and logs transaction details in the Clearing House.
2) **Intermediary Participants**: Trusted entities in charge of establishing trust, providing metadata descriptions, and creating business models around offered services.
   - Broker Service Provider: Maintains a repository of data sources within IDS, offering an interface for submitting and retrieving descriptive metadata.
   - Clearing House: Manages data transaction services within the IDS, ensuring accurate logging for billing purposes and data transfer validation [25].
   - Identity Provider: Entity responsible for creating, managing, and validating identities within the IDS. This includes a Certification Authority (CA) to issue digital certificates, a Dynamic Attribute Provisioning Service (DAPS) to attach properties, and a Dynamic Trust Monitoring (DTM) for enhanced network security.
   - Vocabulary Provider: Oversees the management of data models and metadata elements for the proper annotation and description of datasets in the IDS.
   - App Store Provider: Distributes Data Apps, providing tools for data processing workflows.
3) **Service Providers**: IT entities providing Software as a Service (SaaS), encompassing hosting infrastructure and data services for data quality enhancement and supplying software essential for IDS connector functionalities based on agreements between providers and consumers.
4) **Governance Body**: Entities collaborating on the certification processes of IDS components and participants.

The IDSA is developing the Dataspace Protocol (DSP) [26], which is becoming the basis for the technical development of the Eclipse Dataspace Components (EDC) [1]. The protocol defines component interactions and is the technical specification for the IDS RAM. It is divided into four domains:

[1]https://github.com/eclipse-edc

1) Data space model and terminology: Creates the foundation for interoperability among participants through defined ontologies and taxonomies.
2) Catalog protocol: Data description and retrieval, adhering to the Data Catalog Vocabulary (DCAT) [27].
3) Contract negotiation protocol: Delineates the interactions for establishing mutually agreed contracts, ensuring that terms of access and control rules are consented, framed by the Open Digital Rights Language (ODRL) [28].
4) Transfer process protocol: Details the data transfer procedure post-contract agreement, focusing on the states of the transfer rather than the protocols used.

III. Related Work

Research in the data space domain is actively exploring the integration of Internet of Things (IoT) devices with DLTs to facilitate the adaptation of data spaces to IoT environments. This includes leveraging communication protocols for automated data exchange processes [29][30]. Concurrently, the potential of blockchain to reinforce the IDS RAM architectural concepts is recognized, with the IDSA examining its application in data storage and cataloging. Blockchain's application within the IDS is debated on [31] in implementing:

- **Identity Provider**: This involves linking the ledger and the IDS connector environment using the same certificate schema, with blockchain technology as the Identity Provider based on decentralized identity management.
- **Broker Service Provider**: The registry of connectors and their available data offerings can be listed on the blockchain. However, the immutable nature of DLT presents a challenge for modifying offerings, as new offers must be uploaded for any change.
- **Clearing House**: While passive monitoring technologies like Policy Enforcement Point (PEP) deliver events indicating data usage, the logs can be stored on a blockchain.

Further extending the potential roles of blockchain in data spaces, Prinz et. al [32] have considered using blockchain for storing smart contracts, which can dictate actions within a data space according to the defined rules, facilitating authorization and control of access and usage. Moreover, the Data Spaces Support Centre (DSSC) blueprint document [33] also points out the potential use of blockchain for decentralized identity management and storage of participants' identities.

Practical applications of DLT in actual data spaces have been presented without delving into the technical specifications of their nature or exact implementation. For instance, the use of blockchain is noted by Meneguzzo et. al [34] [35] to implement a data catalog of energy datasets, while the actual data transfer and control processes are performed via connectors. Similarly, adopting an unspecified type of DLT for exchanging information regarding threats or cyber-attacks on critical infrastructure is covered by Sayad et. al [36].

This work addresses the gap between theoretical blockchain studies and practical applications by focusing on a DAG-based DLT like IOTA's Tangle, particularly suited for IIoT environments. Unlike previous research that overlooks the practical implementation and benefits of alternative DLT types, this work implements specific architectural components within the IOTA framework, such as an Identity Provider,

Broker Service Provider, Clearing House, and a wallet service for secure transactions. Additionally, it tackles practical challenges within data spaces, such as onboarding, data offerings, and exchange procedures, aiming to create a data-sharing ecosystem for the secure exploitation of machine data.

IV. Processes for IIoT Data Exploitation

This work focuses on securely sharing machine-generated data, applying the architecture and protocols outlined by the IDSA to the IOTA ecosystem, adapting the processes described on the Process Layer of the IDS RAM [8]:

- **Onboarding**: Adjusted to encompass the registration, identification, and management of participants within a data space, extending beyond the original scope of connector provision and certification.
- **Data Offering**: This involves describing data assets using the DCAT ontology, outlining usage policies with ODRL, and specifying pricing within the service catalog.
- **Contract Negotiation**: Concentrates on negotiating contract terms between data consumers and providers, highlighting the automation of parameter negotiation and formulating the final contract as critical challenges.
- **Exchanging Data**: This work adopts a decentralized model where each participant maintains their own DLT for data storage. It focuses on ensuring secure access through access control mechanisms and PEPs, with IOTA's DLT employed for storing participant data.
- **Policy Enforcement**: Pertains to the technical enforcement of data usage policies related to data assets, especially concerning the consumer and end-user side, to guarantee correct and compliant data usage.

While the IDS RAM acknowledges the potential development of Data Apps, this initial phase of this work does not include them. However, there is scope for incorporating such functionality through Data Apps in future work.

V. Proposed Architecture

The proposed architecture, as illustrated in Figure 3, integrates three core services within a data space: an Identity Provider, a Broker Service Provider, and a Clearing House. These services are based on the SSI concept and constitute the control plane of the architecture. This plane implements a decentralized identity management system for participant, component, and service identification. It is enabled by an IOTA Tangle DLT common to all participants, managing identities and ensuring traceability, acting as the verifiable registry of interactions across components.

Participants in the data space have the flexibility to select their preferred data storage solutions, ranging from traditional databases to various types of DLTs. However, an IOTA Tangle DLT has been specifically chosen for this proposal for the data plane. This network securely manages data storage, ensures data provenance, and maintains traceability, with access strictly controlled and granted only under agreed conditions.

This setup orchestrates a secure data flow, from storing machine-generated data in the Tangle, cataloging these data assets, negotiating contract terms between data consumers and providers, and culminating in the secure data exchange. Access to data stored in the Tangle is governed by access controls and policies, ensuring compliance through policy enforcement. Specifically, the process unfolds as follows: (*1*) Machine-generated datasets are stored on the Tangle, each tagged with a DID linked to the originating machine for data provenance. (*2*) Data owners authorize connectors to publish descriptive metadata for their datasets, involving interactions with the Identity Provider for registration and DID assignment, followed by VC generation for metadata, policies, and pricing, utilizing the Tangle for identity verification. (*3*) Data owners sign the VC, producing a VP published on the Metadata Catalog as a data offering. (*4*) Publications are logged on the Tangle by the Clearing House for transparency.

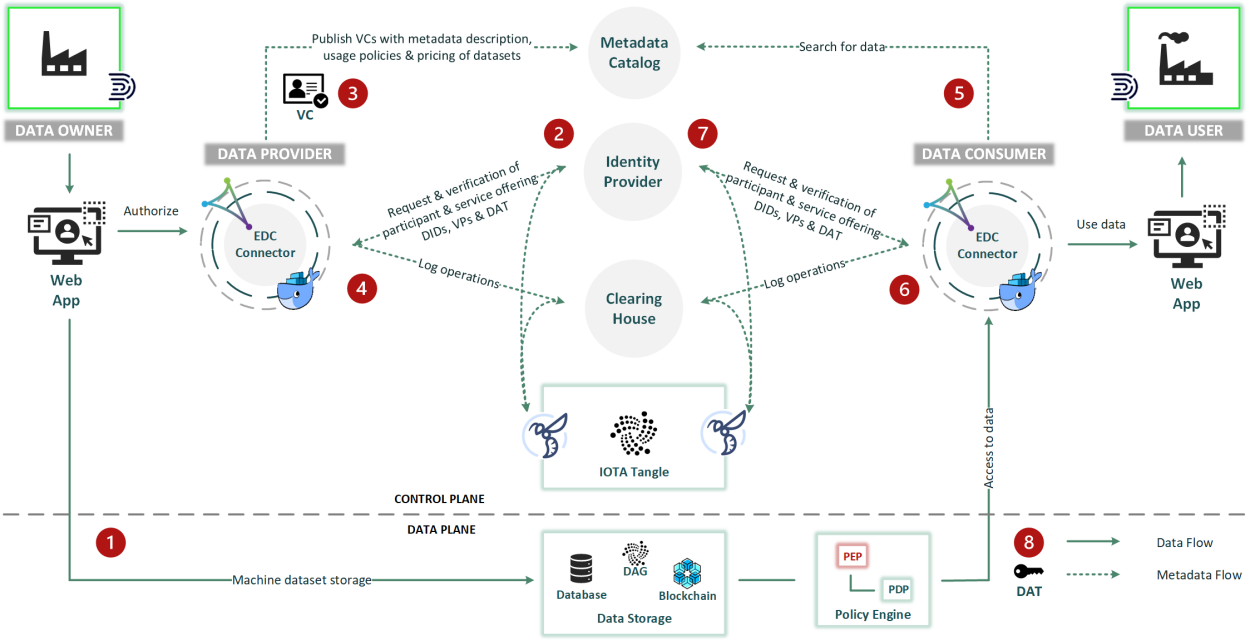

Figure 3: Proposed architecture for the IDS RAM implementation in the IOTA ecosystem

(*5*) Data users search for datasets via the connector, querying the Metadata Catalog by topics. (*6*) Search operations are audited by the Clearing House, recording all transactions on the Tangle. (*7*) Negotiation of contract terms follows, leading to a Dynamic Attribute Token (DAT) generation upon agreement. (*8*) The DAT enables data retrieval from the Tangle, with access and usage regulated by PEP, Policy Decision Point (PDP), and DAT validation.

This interaction between the control and data planes ensures that data sharing adheres to the principles of security, transparency, and data sovereignty, main features of the IDSA. Delving into the control plane of the architecture, the following sections detail the characteristics of the core components.

A. Identity Provider

This component is the identity enabler of the IDSA architecture, marking a shift from the association's standard centralized X.509 certificate-based identity management towards a decentralized model grounded in SSI. This evolution strengthens the fundamental decentralization principles of DLT applications, focusing on data sovereignty and enhancing participant autonomy in the data space. By adopting a decentralized identity management approach, the proposed architecture harmonizes with initiatives like Gaia-X [22].

The main functionalities of this component include the following: (1) issuance, management, and validation of DIDs linked to every data space participant, technical component, and offered datasets or services, (2) issuance, semantic and syntactic validation of VCs, along with the generation and validation of VPs for description of data offerings, and (3) issuance of DATs for data access control.

B. Metadata Catalog

The Metadata Catalog, acting as the Broker Service Provider within the IDSA architecture, facilitates searching and querying data within the data space. It displays VPs that include metadata descriptions, usage policies in ODRL format, and pricing details. The structure of VCs positions the data owner as the offer holder and the infrastructure administrator as the credential issuer, who serves as the trust anchor in the ecosystem. As part of this secure environment, access links to the data are revealed only after the parties reach an agreement. Furthermore, publishing a data offer triggers the logging of essential details, such as a hash of the complete dataset and a link to the catalog, in the Tangle through the Clearing House to ensure data transparency and traceability.

Each participant must maintain a local VC wallet, which ensures personal control and secure storage of their credentials. In contrast, VPs, which are VCs signed by the holder to describe data offerings, are made publicly available in the Metadata Catalog through the cataloging service. This setup guarantees that while the VC wallet offers secure, localized storage for credentials, VPs allow public access to the descriptions of data offerings.

In the preliminary stages of this research, the Metadata Catalog is configured as a global entity accessible to all participants within the data space, serving as a unified point of interaction. However, a decentralized approach can also be conceptualized, in which individual providers manage their own metadata catalogs that host VPs specific to their data offerings. In this decentralized framework, a global Metadata Catalog would aggregate selected VPs from these provider-specific catalogs, selectively making information publicly accessible. This architecture would support a distributed storage model where data is held within provider-controlled zones, augmented by a generalized, aggregated layer to facilitate broader access, aligning with the principles of data sovereignty and controlled data sharing.

When enhancing the descriptive VPs for data offerings based on the DCAT standard, it is crucial for all ecosystem participants to adopt a standardized data offering format consistently. This standardization ensures that data is formatted in a universally understandable and operable manner, facilitating the grouping of similar data types. However, the current system lacks a Vocabulary Provider, a key component for achieving full interoperability within the ecosystem. Integrating a Vocabulary Provider in future updates would enable support for various data formats and improve seamless communication and data exchange across different entities.

C. Clearing House

The Clearing House component within the proposed architecture is critical for recording and monitoring operations throughout the data space, directly interacting with the underlying Tangle network nodes to store these logs. It records all activity in the data space, including: (1) participant registration, (2) data offering publications, (3) data asset searches, (4) contract negotiations, and (5) data access and usage control. These records provide transparency and facilitate the monitoring of policy compliance and data exchange billing within the data space, leveraging the initial platform's payment system for data usage billing.

Furthermore, while the Clearing House meticulously records and stores every transaction, it operates under strict access restrictions. Access to this data is limited only to defined services or as required by specific operational needs, ensuring a balance between transparency and data privacy.

VI. Implementation

This section showcases the implementation of various processes and interactions among components and participant roles within the proposed architecture for the defined IIoT

```
{
  "@context": {
    "edc": "https://w3id.org/edc/v0.0.1/ns/"
  },
  "@type": "PolicyDefinition",
  "policy": {
    "@context": "http://www.w3.org/ns/odrl.jsonld",
    "@type": "Set",
    "duty": [
      {
        "target": "http://localhost:8091/asset:12",
        "action": "use",
        "constraint": {
          "leftOperand": "location",
          "operator": "eq",
          "rightOperand": "EU"
        }
      }
    ]
  }
}
```

Figure 4: Structure of ODRL usage policies definition

scenario. It includes a sequence diagram in Figure 5 illustrating the overall flow of interactions within the data space.

Table I reflects the details of the components described for the control plane of the proposed architecture, including different IOTA frameworks and deployment solutions, as well as the main processes they are involved in. In addition, Table II compares the current state of implementation for each identified process, accompanied by proposed solutions.

The control plane is anchored on a private IOTA Tangle network consisting of multiple Hornet nodes. In this configuration, the DID documents associated with participant identities are stored as Alias Outputs. At the same time, records from the Clearing House are stored as Basic Outputs, encapsulating data within their metadata field. In addition, a separate IOTA network is used for data storage within the data provider's data plane, where machine-generated data is also stored in transactions categorized as Basic Outputs. To implement the data space, the architecture uses EDC connectors, chosen for their modular design and compatibility with the IDSA's DSP [37]. These connectors are implemented within the Minimum Viable Dataspace (MVD) scenario.

Regarding processes, the onboarding is successfully implemented using a decentralized management identity system based on SSI that identifies all participants in the data space with their DID, allowing for the assignment of properties or attributes in the form of VCs, implemented by the IOTA Identity framework. As part of policy enforcement, the system relies on logs from the Clearing House to ensure traceability. These logs are stored on the IOTA network using the IOTA Client and IOTA Wallet frameworks for storing data encapsulated in transactions, which are also integral to the secure payment system. Additionally, the data offering process, including the description of data and its publication in the data catalog, is effectively implemented using MongoDB to store the data offerings. Furthermore, the data transfer process facilitates controlled access to data stored on the Tangle, which occurs after verification of the assigned token. However, as this research work is currently under development, efforts are ongoing in the following key areas:

Table I
Implementation details and involved processes of the proposed architecture's control plane

Component	Implementation	Processes
Identity Provider	IOTA Identity	Onboarding, Data Offering
Metadata Catalog	MongoDB	Data Offering
Clearing House	IOTA Client, IOTA Wallet	Policy Enforcement
Connector	EDC Connector, Minimum Viable Dataspace[1]	All
DLT	Private IOTA Tangle, Stardust version[2], Alias Outputs[3], Basic Outputs[4]	Onboarding, Data Offering, Contract Negotiation

[1] https://github.com/eclipse-edc/MinimumViableDataspace
[2] https://github.com/iotaledger/hornet/tree/develop/private_tangle
[3] https://wiki.iota.org/tips/tips/TIP-0018/#alias-output
[4] https://wiki.iota.org/tips/tips/TIP-0018/#basic-output

Table II
Implementation status of data spaces integration with IOTA

Process	Description	Proposed Solution	State
Onboarding	Grant access to IDS as data consumer or provider	Decentralized identity management through SSI	Complete
Data Offering	Description of data assets and usage policies	VCs for asset description, published via VPs	Complete
Contract Negotiation	Negotiation of data usage contract terms	Automated tools for contract terms negotiation	Ongoing Work
Exchanging Data	Provide access to data stored in the Tangle	Using DAT-based control access	Complete
Policy Enforcement	Technical enforcement of usage policies	PEP integration, leveraging smart contracts	Ongoing Work

A. Contract Negotiation

According to the DSP specification, the negotiation process within the data space is currently facilitated through human-mediated solutions, which are suitable for handling personal data where terms are set by the end-user. However, industrial machines have a clear opportunity to transition to a more automated system. Starting with an initial description of policies based on ODRL, the focus is on aligning offer and demand through policy matching, rather than simple comparison. This move towards automation is especially beneficial in environments dominated by non-personal, machine-generated data, where policy-driven negotiations can substantially enhance the efficiency and precision of stakeholder agreements.

Establishing a dynamic negotiation environment is crucial for the iterative refinement of terms based on pre-defined policies until a mutual agreement is reached. By embedding the negotiation phase within smart contracts on a DLT, this approach ensures that agreements are both automated and enforceable, aligning closely with stakeholder needs. Furthermore, this strategy adheres to initial policy mapping, making the negotiation process a central element in achieving consensus between providers and consumers. Building upon the manual comparison of ODRL policies as proposed in [38], this work seeks to automate the negotiation process further, thereby enabling more efficient contract terms negotiations.

B. Policy Enforcement

The concept of policy enforcement in the IDS RAM underlines the need for mechanisms to ensure that data remains under the owner's control, facilitating sovereignty and compliance during user access. This approach is central to monitoring data use, ensuring compliance with agreed terms, and managing non-compliance. The IDSA tackles this challenge, as detailed in [39], by advocating for the use of technical enforcement mechanisms. Notably, MYDATA [2] enables defining policies that restrict data access frequencies, specify allowable access time frames, and delineate access based on geographical location, thus providing the technical enforcement of such policies. Moreover, IDSA also introduces

[2]https://git.iese.fraunhofer.de/mydata/sdk/-/tree/master?ref_type=heads

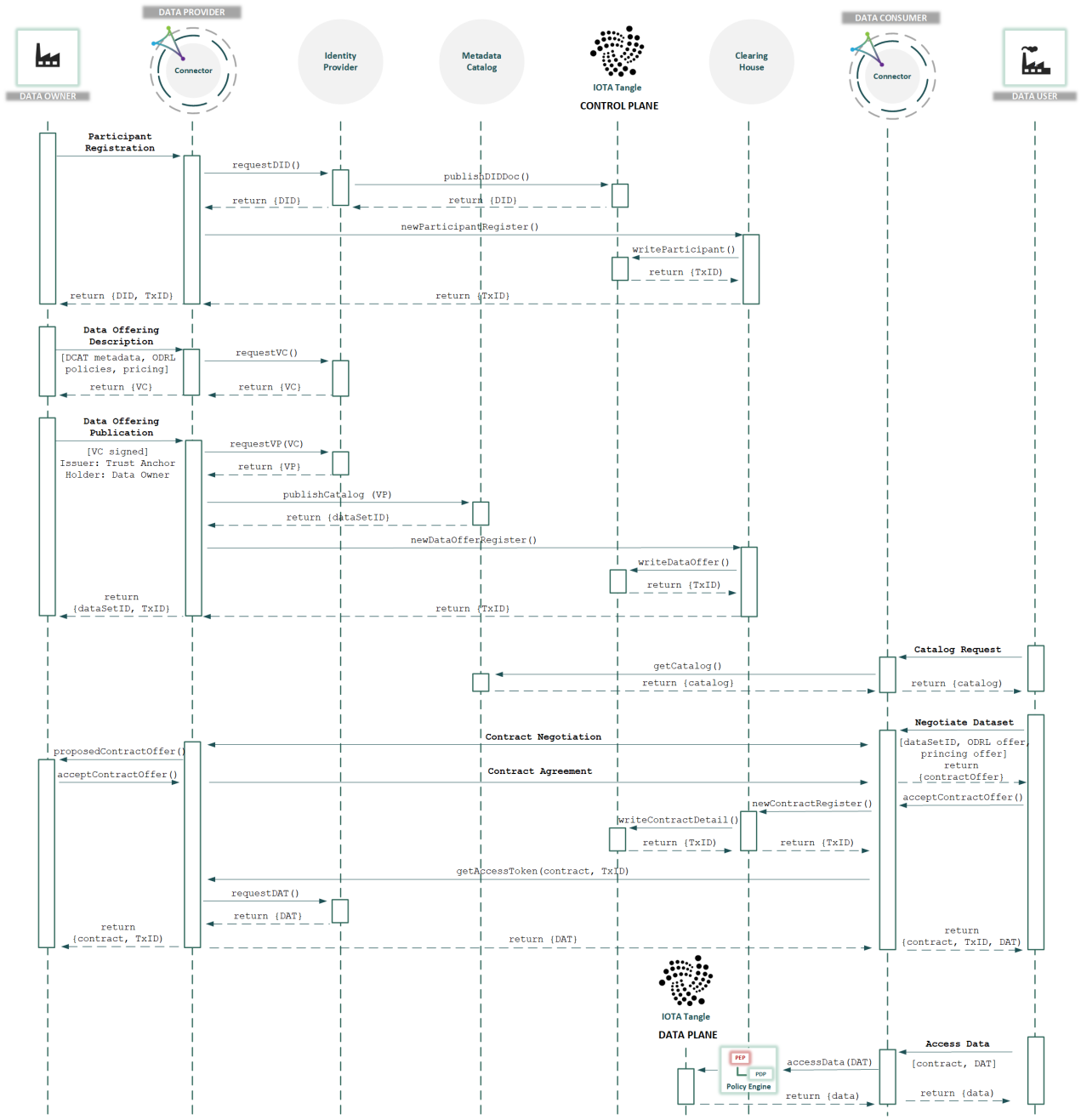

Figure 5: Participant onboarding, data offering, contract negotiation and data exchange processes in the IOTA-based data space

the LUCON policies [40] to manage data flows by dictating the routing of messages across services.

Gil et al. [41] propose a methodology for determining the most suitable solution for implementing Distributed Usage Control (DUC). Options for deploying a policy control system include within the connector, as initially proposed by IDS RAM, as an external system, or even integrated directly with the IOTA network as Denis et al. propose in [42], ensuring that the integrity of data usage is maintained over time. In addition, smart contracts can be used in conjunction with these solutions to track data lifecycle events back to the point of acquisition by the user, addressing the challenges of policy compliance and unauthorized data sharing after acquisition.

VII. Conclusion and Future Lines

This work presents the practical integration of the IDS RAM conceptual framework with the IOTA architecture, stepping beyond theoretical discussions to implement a DLT solution tailored for the IIoT data space ecosystem. Unlike traditional blockchain-focused studies, this work leverages IOTA's DAG structure to implement core IDS components, including an Identity Provider, a Metadata Catalog, a Clearing House, and a wallet service for value transactions, significantly enhancing the security and utility of the ecosystem for third-party data use. Grounded in the roles and concepts of IDS and adopting a decentralized interconnection approach followed by initiatives such as Gaia-X, this work marks an

advancement in secure, interoperable, and efficient data management within the IIoT domain, demonstrating the benefits of integrating IDS with the capabilities of the IOTA framework.

As future work, the project aims to implement and automate contract negotiation and policy enforcement processes. The integration of a Vocabulary Provider is intended to achieve full interoperability, enhancing the platform's ability to facilitate common understanding across systems and stakeholders. At the same time, the introduction of a Data App Provider will add modularity by incorporating advanced data handling capabilities that can be tailored to specific needs. These strategic enhancements will be evaluated in simulated and real-world environments to ensure that the system effectively meets operational requirements and maintains robustness and reliability in the evolving IIoT domain.

ACKNOWLEDGMENTS

This work has been financed by the European Commission through the Horizon Europe program under the HAVEN project (grant agreement number 101137636). It was also partially supported by MCIN/ AEI /10.13039/501100011033/ FEDER "Una manera de hacer Europa" under the grant PID2021-124502OB-C44 (PRESECREL).

REFERENCES

[1] N. Schmidt and A. Lueder, "The Flow and Reuse of Data: Capabilities of AutomationML in the Production System Life Cycle," *IEEE Industrial Electronics Magazine*, vol. 12, pp. 59–63, 6 2018.

[2] L. D. Nguyen, A. Bröring, M. Pizzol, and P. Popovski, "Analysis of distributed ledger technologies for industrial manufacturing," *Scientific Reports 2022 12:1*, vol. 12, pp. 1–11, 10 2022.

[3] S. Y. Popov, "The tangle," 2015. [Online]. Available: https://api.semanticscholar.org/CorpusID:4958428

[4] A. Raschendorfer, B. Mörzinger, E. Steinberger, P. Pelzmann, and R. Oswald, "On IOTA as a potential enabler for an M2M economy in manufacturing," *Procedia CIRP*, vol. 79, pp. 379–384, 1 2019.

[5] N. Gligoric, D. Escuín, and L. Polo, "IOTA-Based Distributed Ledger in the Mining Industry: Efficiency, Sustainability and Transparency," *Sensors 2024, Vol. 24, Page 923*, vol. 24, p. 923, 1 2024.

[6] A. Kovach, "Sistema descentralizado de gestión de identidades digitales y pagos seguros en entornos IIoT," 2023, Master Thesis, University of Cantabria, Santander, Spain.

[7] T. Uslaender and S. Dalmolen, "IDSA Position Paper Data Sovereignty - Requirements Analyis of Manufacturing Use Cases," *International Data Spaces Association*, 2022.

[8] B. Otto, S. Steinbuss, A. Teuscher, and S. Bader, "IDS RAM 4," *International Data Spaces Association*, 2022. [Online]. Available: https://docs.internationaldataspaces.org/ids-knowledgebase/v/ids-ram-4/

[9] L. T. Khrais, "Comparison study of blockchain technology and IOTA technology," *Proceedings of the 4th International Conference on IoT in Social, Mobile, Analytics and Cloud, ISMAC 2020*, pp. 42–47, 10 2020.

[10] J. Rosenberger, F. Rauterberg, and D. Schramm, "Performance study on IOTA Chrysalis and Coordicide in the Industrial Internet of Things," *2021 IEEE Global Conference on Artificial Intelligence and Internet of Things, GCAIoT 2021*, pp. 88–93, 2021.

[11] W3C, "Decentralized Identifiers (DIDs) v1.0," 2022. [Online]. Available: https://www.w3.org/TR/did-core/

[12] ITU-T, "Security guidelines for using distributed ledger technology for decentralized identity management," International Telecommunication Union, ITU-T Recommendation X.1403, 2020. [Online]. Available: https://www.itu.int/rec/T-REC-X.1403-202009-I/es

[13] W3C, "Verifiable Credentials Data Model v2.0," 2024. [Online]. Available: https://www.w3.org/TR/vc-data-model-2.0/

[14] B. Otto and M. Jarke, "Designing a multi-sided data platform: findings from the International Data Spaces case," *Electronic Markets*, vol. 29, pp. 561–580, 12 2019.

[15] European Commission, "A European Strategy for Data." [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/strategy-data

[16] European Parliament and Council, "Directive (EU) 2019/1024 on open data and the reuse of public-sector information," Official Journal of the European Union, 2019.

[17] European Parliament and Council of the European Union, "Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union," Official Journal of the European Union, 2018.

[18] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," pp. 1–88, 2016.

[19] European Parliament and Council of the European Union, "Regulation (EU) 2022/868 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)," Official Journal of the European Union, no. L 152, pp. 1–44, 2022.

[20] European Parliament and Council of the European Union, "Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)," Official Journal of the European Union, 2023.

[21] S. Steinbuss, "IDSA Rulebook," *International Data Spaces Association*, 2023. [Online]. Available: https://docs.internationaldataspaces.org/ids-knowledgebase/v/idsa-rulebook/front-matter/readme

[22] Gaia-X European Association for Data and Cloud (AISBL), "Gaia-X Architecture Document - 22.04 Release," 2021.

[23] G. Giussani, S. Steinbuss, M. Holesch, and N. Gras, "Data Connector Report," *International Data Spaces Association*, 2024.

[24] S. Bader, J. Pullmann, and C. Mader, "The International Data Spaces Information Model – An Ontology for Sovereign Exchange of Digital Content," *Lecture Notes in Computer Science*, pp. 176–192, 2020.

[25] S. Bader, G. Bramm, and J. Ceballos, "IDSA White Paper Specification IDS Clearing House," *International Data Spaces Association*, 2020.

[26] International Data Space Association, "Dataspace Protocol 2024-1," 2024. [Online]. Available: https://docs.internationaldataspaces.org/ids-knowledgebase/v/dataspace-protocol/overview/readme

[27] W3C, "Data Catalog Vocabulary v.3," 1 2024. [Online]. Available: https://www.w3.org/TR/vocab-dcat-3/

[28] R. Iannella, M. Steidl, S. Myles, and V. Rodriguez-Doncel, "Open Digital Rights Language (ODRL) v.2.2 Ontology," 2017. [Online]. Available: https://www.w3.org/ns/odrl/2/

[29] M. Nast, B. Rother, F. Golatowski, D. Timmermann, J. Leveling, C. Olms, and C. Nissen, "Work-in-Progress: Towards an International Data Spaces Connector for the Internet of Things," *IEEE International Workshop on Factory Communication Systems, WFCS*, 2020.

[30] H. Qarawlus, M. Hellmeier, and J. Pieperbeck, "Sovereign Data Exchange in Cloud-Connected IoT using International Data Spaces," *2021 IEEE Cloud Summit, Cloud Summit 2021*, pp. 13–18, 2021.

[31] S. Steinbuss, M. Punter, F. Fournier, and I. Skarbovski, "Blockchain Technology in IDS," *International Data Spaces Association*, 2019.

[32] W. Prinz, T. Rose, and N. Urbach, "Blockchain Technology and International Data Spaces," in *Designing Data Spaces*, B. Otto, M. ten Hompel, and S. Wrobel, Eds. Springer, Cham, 2022, pp. 165–180.

[33] Data Spaces Support Centre, "Data Spaces Blueprint v.0.5," 2023.

[34] S. Meneguzzo, A. Favenza, V. Gatteschi, and C. Schifanella, "Integrating a DLT-Based Data Marketplace with IDSA for a Unified Energy Dataspace: Towards Silo-Free Energy Data Exchange within GAIA-X," *5th Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2023*, 2023.

[35] S. Meneguzzo, A. Favenza, V. Gatteschi and C. Schifanella, "Exploring the Potential of Energy Data Marketplaces: An Approach based on the Ocean Protocol," *Proceedings - International Computer Software and Applications Conference*, vol. 2023-June, pp. 1488–1494, 2023.

[36] K. Sayad and B. Lemoine, "Towards Cross-domain Resilience in SDN-enabled Smart Power Grids: Enabling Information Sharing through Dataspaces," *IEEE International Conference on Omni-Layer Intelligent Systems, COINS 2023*, 2023.

[37] T. Dam, L. D. Klausner, S. Neumaier, and T. Priebe, "A Survey of Dataspace Connector Implementations," *ITADAT2023: Italian Conference on Big Data and Data Science*, 2023.

[38] B. Esteves, V. Rodríguez-Doncel, and H. J. Pandit, "Using the ODRL Profile for Access Control for Solid Pod Resource Governance," *Lecture Notes in Computer Science*, vol. 13384 LNCS, pp. 16–20, 2022.

[39] S. Steinbuss, "Usage Control in the International Data Spaces," *International Data Spaces Association*, 2019.

[40] J. Schuette and G. S. Brost, "LUCON: Data Flow Control for Message-Based IoT Systems," *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Trustcom/BigDataSE 2018*, pp. 289–299, 2018.

[41] G. Gil, A. Arnaiz, F. J. Diez, and M. V. Higuero, "Evaluation Methodology for Distributed Data Usage Control Solutions," *GIoTS 2020 - Global Internet of Things Summit, Proceedings*, 2020.

[42] N. Denis, M. Laurent, and S. Chabridon, "Integrating Usage Control Into Distributed Ledger Technology for Internet of Things Privacy," *IEEE Internet of Things Journal*, vol. 10, pp. 20 120–20 133, 11 2023.