ConfMod: A Simple Modeling of Confidentiality Requirements for Inter-Organizational Data Sharing

Jan Pennekamp*, Paul Weiler†, Matthias Bodenbenner†, Maximilian Sudmann*, István Koren‡, Ike Kunze*, Marcel Fey†, Dominik Wolfschläger†, Christian Brecher†,¶, Robert H. Schmitt†,¶, Klaus Wehrle*
*Communication and Distributed Systems, RWTH Aachen University, Germany · {lastname}@comsys.rwth-aachen.de
†Machine Tools and Production Engineering, RWTH Aachen University, Germany
‡Process and Data Science, RWTH Aachen University, Germany · ¶Fraunhofer IPT, Germany

***Abstract*—Exploiting data and information is known to be essential for tapping into unrealized (business) potential. In the context of the Industrial Internet of Things (IIoT), concerns related to the sensitivity of data frequently hinder its sharing (across organizations). Despite this situation, universal approaches that account for and appropriately model the confidentiality needs of stakeholders are still missing. In this paper, we address this research gap by proposing *ConfMod*, a middleware that simplifies the fine-granular modeling of confidentiality requirements while striving for interoperability with other tools and standardization in the area. We evaluate ConfMod in a diverse set of twelve real-world use cases from industry and show its general feasibility. Hence, we are confident that the functionality and simplicity of ConfMod facilitate an important building block for the IIoT, which will fuel inter-organizational data sharing in the future.**

***Index Terms*—Information Security; Information Privacy; Interoperability; Unified Framework; Internet of Production**

I. Introduction

The key drivers of the Industrial Internet of Things (IIoT) include digitalization, broad data collection and analysis, novel types of information modeling and sharing, and knowledge exploitation. As such, they not only fuel Industry 4.0 [1], [2] but also Industry 5.0-related developments [3], [4]. Several large-scale industry and research initiatives, such as AIMS5.0 [4], [5], Arrowhead [6], Internet of Production [7], [8], Physical Internet [9], or Productive4.0 [10], emphasize these trends.

Certainly, access to data and the downstream use of extracted knowledge is already valuable for a single shopfloor. However, more impactful advances can be made when also exchanging information with other organizations [11]. A fully-developed ecosystem would correspond to an interconnected IIoT that exchanges knowledge globally across stakeholders while accounting for the stakeholders' confidentiality concerns. Particularly in light of mass customization, i.e., in single-part and small-batch production, data exchange with regard to first time right is invaluable for solving the conflict between production time, production costs, and product quality [12]. Consequently, participating in data sharing is inevitable for operating a sustainable and competitive business.

Simultaneously, the sensitivity of data, information, and knowledge is a major concern in industry. Reports [13], [14] detail that most data is never shared, primarily due to a fear of negatively impacting data sovereignty but also to maintain a competitive advantage. Currently, industry and research are developing individual solutions for each specific data-sharing use case to meet the respective confidentiality requirements. A single modeling approach that uniformly tackles diverse use cases is missing. Examples include data sharing along supply chains [15], benchmarking companies [16], or exchanging process parameters with competitors [17], [18]. As a result, the underlying approaches are rarely reused these days since use cases usually cover different data-sharing scopes, i.e., which (external) parties are the recipients of data. Some data may be shared with direct suppliers, while other data is only intended for consumers or even uniquely filtered for competitors. In Section II-A, we further elaborate on the different scopes.

Related work, including European data space initiatives, such as International Data Spaces (IDS) [19] and Gaia-X [20], is primarily concerned with regulatory aspects and regulations, e.g., the EU Data Act [21]. These efforts advocate for data sharing and a joint data-driven economy. Other approaches focus on engineering [22] and technical advances [23], [24] while excluding the modeling of arbitrary confidentiality requirements. Hence, altogether, these efforts miss distinct concepts and implementations of privacy and confidentiality measures. The IIoT and Industry 5.0 would greatly benefit from an intermediary that efficiently addresses these aspects with minimal barriers to entry and effortless usability.

Hence, the IIoT is in need of an approach that (a) formalizes/standardizes the modeling of confidentiality requirements for inter-organizational data sharing, and (b) accounts for different "sharing" scopes (internal, suppliers, competitors, ...) to reduce the amount of redundant (research) activities.

To address this research gap, in this paper, we propose ConfMod, a framework that simplifies the **mod**eling of **conf**identiality in the IIoT. This way, data owners can easily configure which information is being shared within which scope, e.g., which entity is permitted to have access, allowing for fine-granular yet intuitive configurations. In addition to simply sharing or not sharing data, ConfMod also supports dedicated post-processing operations that alter data to account for specific confidentiality requirements. ConfMod is compatible with and nicely fits to other efforts [23]–[25] that aim to improve standardization and interoperability in the IIoT.

Contributions. Our main contributions are as follows.

- With ConfMod, we close an important gap and provide a universal tool for conveniently modeling the confiden-

tiality requirements in inter-organizational data sharing. This way, we pave the road for structured approaches that realize secure industrial collaboration [7] in the future.
- By exploring ConfMod with domain experts from twelve use cases in industry, we demonstrate its practical utility.

Open Science Statement. We open-sourced our prototypical implementation of ConfMod along with a real-world use case data (cf. Section II-A) to foster its reuse in the IIoT [26].

II. Motivation and Gap in Tooling

Moving on, in Section II-A, we first discuss the setting and outline the need for a modeling approach. Subsequently, in Section II-B, we provide an overview of related work before outlining the research gap we identified (Section II-C). In this paper, we will use data, information, and knowledge interchangeably. While our work builds on considering the lowest layer "data", the other dimensions (i.e., upper layers) are equally affected when restricting or enabling data sharing.

A. Scenario and the Need for Modeling

Data sharing is essential to advance the IIoT and to exploit all associated benefits globally. In this context, organizational aspects must be considered as well [27]. We believe that a corresponding solution, which captures the confidentiality needs and addresses them appropriately, especially in competitive business settings, is still missing, as we outline next.

Inter-Organizational Data Sharing. Research is well aware of different types of inter-organizational data sharing in the IIoT [28], as we visualize in Figure 1. Specifically, we can define different scopes that capture this diversity:

- Direct business partners of an organization (Tier-1 suppliers and customers, including tool manufacturers)
- In-direct partners (Tier-N suppliers and customers)
- External companies (for example, organizations with similar machines or even competitors), and
- Government entities (sharing may be required by law).

Besides this "abstract" classification, organizations may arbitrarily cluster other organizations into scopes that have similar relevance in terms of data sharing for them. This way, they can efficiently capture their confidentiality requirements.

Confidentiality Requirements. Organizations have concrete data security expectations regarding the safeguarding of their data, which is also expressed through the growing relevance of data sovereignty. First of all, they want to protect sensitive information (also to maintain their competitive advantage, i.e., keeping business secrets private), but they also have to comply with legislation and contracts that regulate and mandate the sharing of data. For others, sharing data is even central to their business model. In any case, they can formulate precise confidentiality requirements regarding their data.

The relevant set of applicable confidentiality requirements differs depending on the scope within which data could be shared (i.e., the recipients) and the exact data at hand. Some sensitive details may not be shared at all, while other data may only be shared after post-processing, e.g., normalizing it, adding noise, or computing the average, to obfuscate sensitive

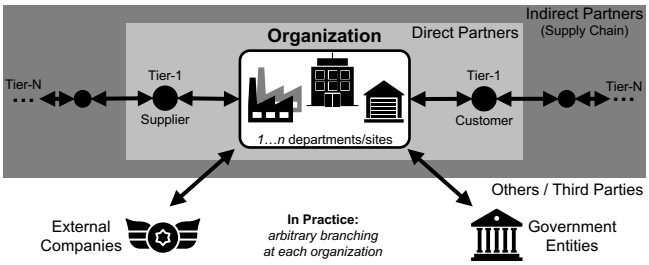

Fig. 1. In the IIoT, we consider different scopes when talking about individual confidentiality requirements. We primarily distinguish sharing within an organization (center) and various forms of inter-organizational data sharing, i.e., direct partners as well as indirect supply chain partners (from left to right) and third parties, such as external companies or government entities.

(contextual) data. Hence, capturing and expressing confidentiality requirements boils down to (i) approving or prohibiting the sharing of data in the first place and (ii) mandating and executing processing steps (if needed) to enable said sharing.

Different from the described data security, we believe that sufficient (best) practices to holistically capture and express data privacy needs have already been developed. In contrast, compiling confidentiality requirements in detail is challenging, often triggered for individual information flows only (no generalization), and does not (yet) follow a standardized form.

Utility for the Internet of Production (IoP). The IoP focuses on the in-depth collaboration of stakeholders in the IIoT. A key component of this approach is the exchange of data, information, and knowledge between different entities along the product development process. The vision of an IoP builds on the idea of the World Wide Lab [8], [29], providing specific domain knowledge in the form of semantic, contextualized data to enable resilient, efficient, and competitive production. Effectively, this development boils down to the establishment of an interconnected system of systems [30], with the vision aligning nicely with other IIoT roadmaps [5].

To illustrate the application potential of a modeling approach in the IoP, we consider an example in milling. Along the production chain of a milled part, a wide range of data is generated: from process planning (3D model of the part, NC program, tool lists, etc.) over the manufacturing process (axis positions, drive currents, force signals from external sensor systems, tool engagement conditions, etc.) to quality assurance (inspection reports, point clouds, etc.) [31]. This data provides valuable insights into the manufacturing process but cannot be shared in full due to reasons such as data privacy, compliance regulations, or the protection of business expertise.

A middleware, which takes relevant confidentiality needs into account, could enable the entire set of process data to be divided into subsets, whose information content and contextual relevance can be defined based on organizational relationships (scopes). While internal data-sharing restrictions primarily pertain to data privacy regulations aimed at protecting personal data—for instance, by removing absolute timestamps from the data to prevent direct identification of machine operators—the restrictions might differ with other organizations involved. For example, a milling tool manufacturer may be granted dedicated insights into user behavior (such as the machine

used, the tools deployed, tool engagement conditions like cutting depth, cutting width, and feed per tooth, as well as spindle current) without revealing information about the underlying manufacturing strategy (e.g., production location, NC program, axis positions and currents, or force signals), thereby safeguarding the company's sensitive know-how.

Accurately modeling the confidentiality requirements of sensitive data could fuel inter-organizational data sharing, thus contributing to collaborative data exploitation in the IIoT.

B. Related Work: Efforts for a Data-Sharing Ecosystem

Prior work primarily touches our research from three angles.

Regulatory. Data space initiatives, e.g., concretized by the IDS [19] and Gaia-X [20], strive for large-scale data sharing and joint data usage while maintaining the data sovereignty of data owners and providers. The core concept of data spaces is the (bilateral) negotiation of individual data usage permissions compared to general usage licenses. Current developments (e.g., [32], [33]) focus on interfaces for exchanging data and contract negotiation while building on organizational security [34]. However, they fall short in configuring and reliably enforcing different levels (or scopes) of confidentiality.

Application. Deploying a uniform confidentiality modeling requires standardized, interoperable data models. Otherwise, the defined confidentiality constraints cannot be mapped automatically to the exchanged data. Typical technologies used in engineering to facilitate interoperability are the Asset Administration Shell (AAS) and OPC UA, which define meta models for structuring process and system data [22], [35]. They even provide technical possibilities for access regulation but do not tackle further confidentiality measures while suffering from high modeling and implementation complexity [36].

Technical. FAIR Sensor Services [37] provide interoperable measurement data via the Sensor Interfacing Language (SOIL) [38], reducing the modeling complexity, while lacking an integration of confidentiality measures. The same holds for FactDAG [25], which allows for tracking the provenance of shared and reused data, Model in the Middle (MitM) [23], [24] (interoperability concept), and the AIMS5.0 AI Toolbox [39], which focuses on sharing AI models with third parties. Zhang et al. [40] propose algorithms to ensure privacy when data is shared among competing parties. However, their work is designed for security experts and requires an individual configuration for each data-sharing process, impairing its scalability.

C. Research Gap: Ease Capturing of Confidentiality Needs

Despite the benefits within reach [11], the IIoT is missing a standardized and universal approach for configuring the confidentiality requirements in the context of (inter-organizational) data sharing, as also pointed out by Neubauer et al. [36]. Having such an approach available would contribute to several advances. First, it would simplify data-sharing practices for organizations because they can reliably express, model, analyze, and ensure information security—(unresolved) confidentiality concerns still hinder inter-organizational data sharing. In addition to supporting confidentiality configurations per scope, a usable approach also makes the general topic more accessible and potentially enables stakeholders to better understand the implications of sharing or not sharing (post-processed) data. Second, it would allow for meta-analyses that highlight which use cases, domains, and settings share similar confidentiality requirements, likely easing the reuse or adaptation of approaches. This way, corresponding information security advances could tackle issues on a bigger scale and move from use case-specific solutions to more universal concepts.

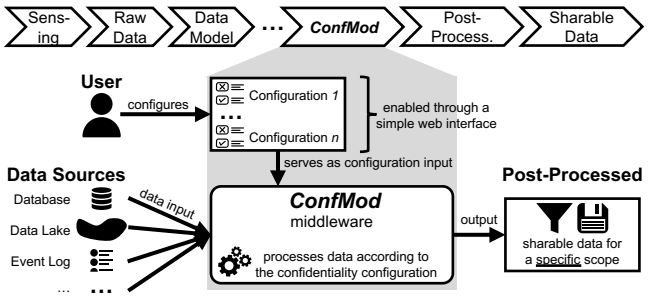

Fig. 2. Our approach is unintrusively embedded in the traditional data processing pipeline, from sensing to sharing. Users interact with ConfMod to configure the confidentiality requirements on a per-scope basis. Our middleware takes different data sources and configuration files as input to process and post-process data according to the confidentiality requirements.

III. ConfMod: Modeling Confidentiality Requirements in the Industrial Internet of Things

We now present ConfMod, our approach for simplifying the modeling of confidentiality requirements. To this end, we first outline the key idea in Section III-A. Afterward, in Section III-B, we elaborate on the different aspects ConfMod can model. Finally, in Section III-C, we outline how users, e.g., industry professionals, would interact with this middleware.

A. Key Idea and Design Overview

To address the outlined research gap (cf. Section II-C), we have developed ConfMod, a middleware for modeling the confidentiality requirements of organizations in the IIoT that maintains interoperability with other tooling (e.g., MitM [23], [24], FactDAG [25], and other downstream analysis pipelines) by using a standardized data model as input and outputting interoperable information. This way, it complements and is unintrusively embedded in the traditional data processing pipeline, from sensing to sharing, as we visualize in Figure 2.

Interfaces. Central to its operation are its two input forms: (1) different data sources (databases, data lakes, event logs, ...) are being processed according to (2) a user-supplied confidentiality configuration. Users interact with the middleware through a simple web interface, which enables them to create and maintain configurations for different scopes (cf. Section II-A). These scopes are not fixed and can be defined as needed (e.g., for sets of organizations), offering flexibility. ConfMod processes the data sources according to the supplied configuration. If marked in the configuration, this step also applies post-processing (e.g., normalization) to hide or remove sensitive details from the output. Eventually, the user receives sharable, interoperable data for a specific scope. By defining

Listing 1. Exemplary YAML configuration (per scope) when using ConfMod.

```yaml
---
metadata: set(key, value)          # high-level metadata
observations:                      # set of observations
  - observation1:
    - metadata: set(key, value)
    - features:                    # set of features
      - feature1:
        - feature: key, value
        - metadata: set(key, value)
# arbitrary many features and observations supported
---
```

precise accessibility rules with an interoperable and reusable data model, ConfMod contributes to FAIR data [41].

Configurations. For each scope, a configuration allows for dealing with general metadata that describes all associated data. Moreover, ConfMod supports an unlimited number of observations. An observation then holds features as well as corresponding feature metadata to comply with the best practices of FAIR data [41]. We summarize this concept in Listing 1. A configuration itself does not hold any data; it only tracks confidentiality requirements for information stored in the selected data sources. Information that is not configured for sharing is not part of an exported configuration, i.e., ConfMod utilizes an opt-in approach and does not leak details about the entire set of theoretically-available information.

Simplicity and Ease of Use. ConfMod is a very simplistic yet unified approach for dealing with confidentiality requirements to (i) not overwhelm users, (ii) allow for great extensibility, e.g., if additional aspects (cf. Section V) must be covered as well, and (iii) be universal, i.e., every data-sharing setting and use case in the IIoT should be supported.

B. Fundamental Modeling Properties

Internally, we rely on a tree-based data structure, as shown in Listing 1, which holds key-value pairs, to fine-granuarly model the mentioned metadata, observations, and features. The top-level metadata covers details that are relevant for all data at hand. In contrast, observations allow for grouping and categorizing data. Each observation then consists of features (which may also hold timeseries data) and metadata for describing the feature in detail, including the type of data. In principle, ConfMod also supports a layered approach per scope to represent and model hierarchical structures. For simplicity, we omit this aspect in our current prototypical realization [26].

Additionally, ConfMod further permits linking fields to ontologies to have a set of accepted ontological terms. Overall, the proposed approach is granular and thus rapidly extensible and extendable: By design, scopes, metadata, observations, and features can be added and configured as needed. Likewise, ConfMod is not constrained to certain data types, post-processing options, or connectors to other data sources. Hence, integrating additional functionality is feasible with little effort.

C. Interacting with ConfMod

The interaction with ConfMod takes place through a simple web interface, lowering the barrier for non-security experts, including engineers or supply chain managers in the IIoT. This design choice significantly increases the concept's scalability as no dedicated expert knowledge on modeling or programming is required. Nonetheless, the generic modeling approach also allows for a programmatic integration with other tools and models. Based on a one-time mapping and integration, the data points for which scopes are defined can be extracted from interoperably-described data using standardized information models, such as MitM, SOIL, AAS, or OPC UA. In the long run, standardized data points could be tagged with default configurations (per scope), enabling confidentiality by default.

Relevant scopes can be predefined or manually added by users (as needed) to address arbitrary settings in the IIoT. ConfMod has an interface to import and export configurations in YAML files (cf. Listing 1). This way, we also enable an automated parsing, processing, and visualizing of different configurations. By integrating the middleware with the post-processing module (cf. Figure 2), confidentiality requirements can be directly applied to the data prior to any sharing.

IV. Real-World Exploration

We now evaluate ConfMod. In particular, we verify whether it addresses the requirements of stakeholders in the IIoT.

A. Prototypical Implementation of ConfMod

We open-source our prototypical realization of ConfMod [26]. In brief, we support all standard data types, including timeseries data and utilize ISO 8601 to represent date- and time-related information. Internally, we use JSON objects (within an SQL database), but we export the configurations in the machine- and human-readable YAML format, enabling convenient processing and interactions. Our frontend, i.e., the web interface, builds on Angular and communicates with the Python backend using the FASTApi web framework.

As post-processing operations, we currently offer the selection of several functions, i.e., rounding, clamping, filtering, normalization, noise, averaging, ensuring k-anonymity, sharing only the distribution, and encryption requirements such as homomorphic encryption, to accommodate diverse use cases.

B. User Study in the Internet of Production

During our evaluation of ConfMod, we pursued two primary goals: (i) modeling real-world use cases, and (ii) assessing the supported features of our approach in light of real-world requirements. Altogether, we were in contact with several experts with different backgrounds. Collectively, these interviews allowed us to model 12 use cases in ConfMod. These use cases cover various areas and applications in the IIoT, including machine tools, injection molding, textile engineering, supplier ratings, the distribution of commercial vehicles, and industry benchmarking, among others. Their data concerns machines, materials, processes, products, supply chains, and surveys, i.e., it is very diverse in nature. Consequently, we cover a wide variety of relevant use cases with highly-individual needs.

We opted for a semi-structured interview process (one hour per use case) to explore which aspects the experts cared about most. That is, we did not prepare a predefined questionnaire but rather compiled a list of high-level discussion points.

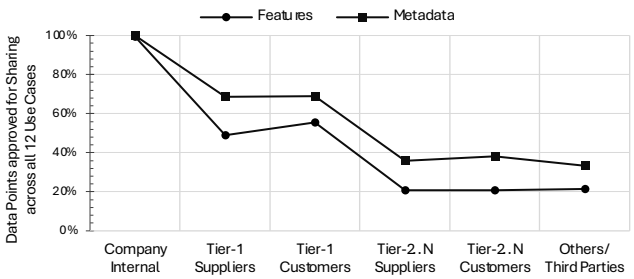

Fig. 3. Our user study confirms that organizations have varying confidentiality requirements depending on the recipient (scope) of data and the involved use case data. They consider metadata to be slightly less sensitive when it comes to sharing it. ConfMod facilitates modeling these nuances and differences.

User Study Remarks. During these interviews, we also collected feedback about the features ConfMod supported at that time. Most commonly, our use case experts requested that we should distinguish direct suppliers and direct customers from each other to account for their differences. Moreover, three participants highlighted the importance of an additional governmental scope to also capture data sharing that must take place for regulatory purposes (if leeway is permitted by law).

Configuration Breakdown. Figure 3 summarizes how the experts configured their data-sharing requirements. Except for a single productivity feature, all agreed to share data within their organization without reservation (no post-processing needed). Across the other scopes, we notice that more than 40 % of data should not be shared at all, with metadata being rated slightly less sensitive. As expected, confidentiality concerns were most prominent when sharing data outside of the supply chain. Interestingly, the confidentiality requirements were not consistent across all scopes, i.e., certain quality criteria were approved for anonymous, anonymized sharing but were considered too sensitive for their (direct) customers.

For the post-processing, normalizing timeseries data for direct partners (or even internally) or numerical values for Tier-N partners were common practices across our use cases. For Tier-N partners, the experts also frequently subsampled timeseries data to reduce the level of detail in shared data.

Overall, we received very positive acclaim for the idea and realization of ConfMod from the participating experts. However, by choice, our selection is slightly biased by only consisting of experts who are generally open to inter-organizational data sharing. The modeling use cases that do not permit any sharing would have resulted in dull/empty configurations.

C. Discussion and Link to other Tools

Now, we discuss ConfMod's achieved utility in more detail.

Security Considerations. Given that ConfMod handles the confidentiality requirements of sensitive data, we also need to account for sensitive information within created configurations. Specifically, we prevent unintended disclosure about theoretically-available data by only including the modeled requirements for data that is being shared in the YAML file. This way, exported configurations do not reveal anything about restricted information, i.e., configurations can be shared with recipients (e.g., to complement discussions) since they do not disclose any extra sensitive details beyond what is shared.

Utility of ConfMod. Our work enables stakeholders to handle their data in a structured manner that is tailored to their organizational relationships and level of trust. The authority and sovereignty over deciding which information is shared, to what extent, and in which context remains entirely with the organizations themselves. Coupled with monetary compensation, this situation could introduce incentives to share data.

In the context of our example (cf. Section II-A), a tool manufacturer could receive information about the usage behavior of a milling tool without being able to infer details about the manufacturing strategy, the geometry of the part produced, or the organizational relationship involved. A tool manufacturer can use this information about the user behavior as feedback for the optimized, needs-based design of new milling tools, on the one hand, and for the targeted provision of optimal tool engagement conditions, on the other hand, to enable resource-efficient milling processes. ConfMod facilitates such an inter-organizational exchange of knowledge through dedicated configurations and post-processed datasets. In manufacturing—particularly in the process design phase, which heavily relies on expert knowledge—corresponding datasets can be used to achieve an efficient and sustainable process design [29].

This way, ConfMod promotes a better understanding and clustering of confidentiality requirements, which can ultimately also contribute to (i) identifying approaches for reuse and (ii) coming up with universally-applicable concepts and designs for confidentiality-preserving data sharing in the IIoT.

Interplay with other Processes. Apart from its compatibility with other concepts like FactDAG, MitM, or SOIL by using a joint terminology for modeled concepts ConfMod might introduce benefits for research data management (including the preparation of artifacts). Specifically, it simplifies the process of selectively sharing data with different stakeholders. Research-specific scopes (e.g., funding organizations, medicine agencies, or collaborators) for providing research data or software could be integrated into data management plans and significantly increase the accessibility and transparency of the conducted research, even beyond applications in the IIoT. Hence, ConfMod aligns nicely with the step of "Data Analysis & Retrieval" in research cooperations [42] and further has positive implications for the "Dissemination" [42].

V. Conclusion and Future Work

Now, we wrap up this paper while putting our research into perspective. That is, we also try to assess ConfMod's impact.

Conclusion. With ConfMod, our interoperable middleware, we address the lack of a tool that allows for the modeling of confidentiality requirements per scope in the IIoT. The successful application to twelve real-world use cases underlines its simplicity, ease of use, and fine-granular modeling capabilities. With this effort, we strive to boost data sharing and reuse of proposed confidentiality-preserving concepts in the IIoT.

Future Work. Moving on, we plan to make our implementation more robust, support additional data sources (cf.

Figure 2), implement an authentication mechanism to restrict access to ConfMod, and introduce a tag system to easily link different features (and possibly metadata) with each other. Additionally, we further want to plot handled configurations to provide a visual aid when comparing the different scopes and their configurations with each other, also across organizations.

Feature-wise, we further want to explore the use of annotations. First, concerning data protection (laws), ConfMod could display which information is allowed to be shared (e.g., to appropriately consider personal data). Second, incorporating legislative requirements could further improve the utility of ConfMod. For example, the Supply Chain Act [43] mandates organizations to provide and share certain information.

Down the road, once data-sharing approaches have further matured, ConfMod could be extended to also support data usage control annotations and, thereby, significantly boost its support for and compliance with data sovereignty (cf. IDS).

Expected Impact of ConfMod. Given the standardized representation, ConfMod allows research to decrement redundant realizations for privacy-preserving data sharing because it is easier to identify "similar" confidentiality requirements. Additionally, it provides computer scientists (in particular, information security experts) with a tool that records confidentiality requirements in a standardized manner, reducing the risk of miscommunication (cf. our previous experiences [42]) and incomplete information. Lastly, ConfMod lays the foundation for defining interoperable confidentiality scopes, paving the way for sovereign data sharing in IDS and Gaia-X.

Acknowledgments

Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC-2023 Internet of Production – 390621612.

References

[1] H. Lasi *et al.*, "Industry 4.0," *Bus. Inf. Syst. Eng.*, vol. 6, no. 4, 2014.
[2] A. W. Colombo *et al.*, "Industrial Cyberphysical Systems: A Backbone of the Fourth Industrial Revolution," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, 2017.
[3] P. K. R. Maddikunta *et al.*, "Industry 5.0: A survey on enabling technologies and potential applications," *J. Ind. Inf. Integr.*, vol. 26, 2022.
[4] G. Dimitrakopoulos *et al.*, "Industry 5.0: Research Areas and Challenges With Artificial Intelligence and Human Acceptance," *IEEE Ind. Electron. Mag.*, vol. 18, no. 4, 2024.
[5] G. Dimirakopoulos *et al.*, "On the Way to Realize the 5th Industrial Revolution: Achievements, Challenges and Research Areas," in *IEEE/IFIP NOMS*, 2023.
[6] J. Delsing, *IoT Automation: Arrowhead Framework*. CRC Press, 2017.
[7] J. Pennekamp *et al.*, "Towards an Infrastructure Enabling the Internet of Production," in *IEEE ICPS*, 2019.
[8] P. Brauner *et al.*, "A Computer Science Perspective on Digital Transformation in Production," *ACM TIOT*, vol. 3, no. 2, 2022.
[9] S. Pan *et al.*, "Digital interoperability in logistics and supply chain management: state-of-the-art and research avenues towards Physical Internet," *Comput. Ind.*, vol. 128, 2021.
[10] K. Furmans *et al.*, "Review of models for large scale manufacturing networks," in *SMMSO*, 2017.
[11] B. Otto *et al.*, "Data sharing in industrial ecosystems: Driving value across entire production lines," McKinsey, Tech. Rep., 2020.
[12] M. Moshiri *et al.*, "An industry 4.0 framework for tooling production using metal additive manufacturing-based first-time-right smart manufacturing system," *Procedia CIRP*, vol. 93, 2020.
[13] N. Ulltveit-Moe *et al.*, "Secure Information Sharing in an Industrial Internet of Things," arXiv:1601.04301, 2016.
[14] European Commission, "Data Act: Commission proposes measures for a fair and innovative data economy," Press Release IP/22/1113, 2022.
[15] L. Bader *et al.*, "Blockchain-Based Privacy Preservation for Supply Chains Supporting Lightweight Multi-Hop Information Accountability," *Inf. Process. Manag.*, vol. 58, no. 3, 2021.
[16] J. Pennekamp *et al.*, "Designing Secure and Privacy-Preserving Information Systems for Industry Benchmarking," in *CAiSE*, 2023.
[17] J. Pennekamp *et al.*, "Privacy-Preserving Production Process Parameter Exchange," in *ACSAC*, 2020.
[18] J. Pennekamp *et al.*, "MapXchange: Designing a Confidentiality-Preserving Platform for Exchanging Technology Parameter Maps," in *ACM SAC*, 2025.
[19] B. Otto *et al.*, "Industrial Data Space: Digital Souvereignity over Data," Fraunhofer, White Paper, 2016.
[20] A. Braud *et al.*, "The Road to European Digital Sovereignty with Gaia-X and IDSA," *IEEE Netw.*, vol. 35, no. 2, 2021.
[21] European Parliament and Council, "Data Act," Regulation (EU) 2023/2854, 2023.
[22] M. A. Iñigo *et al.*, "Towards an Asset Administration Shell scenario: a use case for interoperability and standardization in industry 4.0," in *IEEE/IFIP NOMS*, 2020.
[23] L. Tacke Genannt Unterberg, I. Koren, and W. M. P. van der Aalst, "Maximizing Reuse and Interoperability in Industry 4.0 with a Minimal Data Exchange Format for Machine Data," in *Modellierung*, 2024.
[24] I. Koren *et al.*, "Navigating the Data Model Divide in Smart Manufacturing: An Empirical Investigation for Enhanced AI Integration," in *EMMSAD*, 2024.
[25] L. Gleim *et al.*, "FactDAG: Formalizing Data Interoperability in an Internet of Production," *IEEE Internet Things J.*, vol. 7, no. 4, 2020.
[26] J. Pennekamp *et al.*, "ConfMod," https://github.com/COMSYS/ConfMod, 2025.
[27] A. Stocker *et al.*, "Key Success Factors for the Implementation of Digital Technologies in the Context of Industry 4.0," in *IFIP/IEEE IM*, 2021.
[28] J. Pennekamp *et al.*, "Dataflow Challenges in an *Internet* of Production: A Security & Privacy Perspective," in *ACM CPS-SPC*, 2019.
[29] C. Brecher *et al.*, "The Internet of Production: Interdisciplinary Visions and Concepts for the Production of Tomorrow." Springer, 2023.
[30] C. Pardo, R. Wei, and B. S. Ivens, "Integrating the business networks and internet of things perspectives: A system of systems (SoS) approach for industrial markets," *Ind. Mark. Manag.*, vol. 104, 2022.
[31] F. Wellmann, "Data-driven, context-adaptive productivity increase of NC machining processes," Ph.D. dissertation, RWTH Aachen, 2019.
[32] Eclipse Foundation, "EDC Connector," https://github.com/eclipse-edc/Connector, 2021.
[33] A. S. Ahmadian *et al.*, "Privacy-Friendly Sharing of Health Data Using a Reference Architecture for Health Data Spaces," in *eSAAM*, 2024.
[34] J. Lohmöller *et al.*, "The Unresolved Need for Dependable Guarantees on Security, Sovereignty, and Trust in Data Ecosystems," *Data Knowl. Eng.*, vol. 151, 2024.
[35] A. Schlemitz and V. Mezhuyev, "Approaches for data collection and process standardization in smart manufacturing: Systematic literature review," *J. Ind. Inf. Integr.*, vol. 38, 2024.
[36] M. Neubauer *et al.*, "Architecture for manufacturing-X: Bringing asset administration shell, eclipse dataspace connector and OPC UA together," *Manuf. Lett.*, vol. 37, 2023.
[37] M. Bodenbenner, B. Montavon, and R. H. Schmitt, "Model-driven development of interoperable communication interfaces for FAIR sensor services," *Meas. Sens.*, vol. 24, 2022.
[38] M. Bodenbenner *et al.*, "Domain-Specific Language for Sensors in the Internet of Production," in *WGP*, 2020.
[39] G. Hollósi *et al.*, "AIMS5. 0 AI Toolbox: Enabling Efficient Knowledge Sharing for Industrial AI," in *IEEE NOMS*, 2024.
[40] X. Zheng and Z. Cai, "Privacy-Preserved Data Sharing Towards Multiple Parties in Industrial IoTs," *IEEE JSAC*, vol. 38, no. 5, 2020.
[41] M. D. Wilkinson *et al.*, "The FAIR Guiding Principles for scientific data management and stewardship," *Sci. Data*, vol. 3, 2016.
[42] J. Pennekamp *et al.*, "Collaboration is not Evil: A Systematic Look at Security Research for Industrial Use," in *LASER*, 2021.
[43] G. Felbermayr *et al.*, "Designing EU Supply Chain Regulation," *Intereconomics*, vol. 59, no. 1, 2024.