Advances in Knowledge-Based Systems, Data Science, and Cybersecurity Received 16-07-2024; Accepted 1-04-2025; Published 09-04-2025

Security Models Based on Semantic Web Technologies: The Ark Platform Security Modules

Julio Hernandez julio.hernandez@adaptcentre.ie
ADAPT Centre,
Trinity College Dublin (TCD)
Dublin, Ireland

Haula Sani Galadima haula.galadima@ucdconnect.ie
ADAPT Centre,
University College Dublin (UCD)
Dublin, Ireland

Junli Liang junli.liang@adaptcentre.ie
ADAPT Centre,
University College Dublin (UCD)
Dublin, Ireland

Lucy McKenna lucy.mckenna@adaptcentre.ie
ADAPT Centre,
Trinity College Dublin (TCD)
Dublin, Ireland

Rob Brennan rob.brennan@ucd.ie
ADAPT Centre,
University College Dublin (UCD)
Dublin, Ireland

Corresponding Author: Julio Hernandez

Abstract

The Access Risk Knowledge (ARK) Platform is a socio-technical risk management system for organisations vulnerable to operational failure. ARK is based on Semantic Web standards to support data management activities such as data sharing, integration, classification, and retrieval, supporting the development of a data governance approach. Operationally, the ARK platform provides capabilities for performing socio-technical risk analyses and sharing, analysing, and visualising that information between institutions through an intuitive user interface, combining machine learning approaches to classify and suggest concepts. In this work, we explore the security module of the ARK Platform, where access control and sensitive data processing are integrated into the platform, and it explores the extent to which Semantic Web standards could cope with the requirements for cybersecurity risk management systems. The ARK Platform provides mechanisms to extend its functionality, such as integrating new ontologies or taxonomies for a particular domain, organisation

Citation: Julio Hernandez, et al. Security Models based on Semantic Web Technologies: The ARK Platform Security Modules. Advances in Knowledge-Based Systems, Data Science, and Cybersecurity. Research 2025; 2(1):8. Pages- 172-183

or problem. In this sense, the ARK Platform was extended with incident response (IR) capabilities for socio-technical systems analysis by defining a new ontology for cybersecurity control and a taxonomy of cybersecurity concepts based on the ISO 27000 series standard, DPV controls, NIOSH Controls, and Enterprise Risk Management concepts to model IR artefacts, processes, and roles. Additionally, the security module of the ARK Platform was extended with personal data processing and access control mechanisms restricting access to evidence according to user roles where information related to users and projects are securely persisted in a Semantic Web format. As a result, two ontologies for risk management and two taxonomies of risk and cybersecurity concepts that consider ISO and NIST standards have been published as open sources.

Keywords: Semantic Web, Cybersecurity, Information Security, Sensitive Data Processing.

1. INTRODUCTION

The Semantic Web [1], relies on linked open data to connect diverse resources using W3C standards [2], demonstrating success in areas like knowledge extraction, semantic annotation, and digital libraries [3]. Beyond NLP, it also enables the development of security mechanisms through domain-specific ontologies, such as the W3C's Verifiable Credential Data Model [1] for cryptographically secure, privacy-respecting, and machine-verifiable digital credentials [4, 5]. Another example is the Data Privacy Vocabulary [2] (DPV), which supports the interoperable exchange of personal data processing information [6–8].

This work focuses on the ARK Platform[3], a risk governance tool designed for organizations vulnerable to operational failures. It uses the CUBE methodology [9], for socio-technical analysis in clinical risk management. The platform integrates qualitative clinical risk data with quantitative operational data using Semantic Web technologies and W3C standards, creating a unified risk model. This approach transforms human-oriented quantitative data into machine-readable structured data for large-scale evidence collection and analysis. Key components include two ontologies—the ARK CUBE Ontology[4] and ARK Platform Ontology[5]—and three controlled taxonomies for risk and health terminology. Health and safety experts interact with the platform through a web application[6], which supports risk analysis, mitigation, and evidence linking.

Information sharing has become increasingly important in recent years, especially in healthcare [10, 11]. However, the sensitive nature of health data limits sharing, as organizations aim to keep data owners in control. Adhering to regulations like the General Data Privacy Regulation[7] (GDPR) is essential for building trust in systems that handle sensitive information [12]. The ARK Platform addresses these concerns by incorporating a dataspace security model based on Semantic Web technologies that align with GDPR requirements for personally identifiable information (PII).

[1] https://www.w3.org/TR/vc-data-model/
[2] https://w3c.github.io/dpv/2.0/dpv/
[3] https://openark.adaptcentre.ie/
[4] https://openark.adaptcentre.ie/Ontologies/ARKCube/index-en.html
[5] https://openark.adaptcentre.ie/Ontologies/ARKPlatform/index-en.html
[6] https://openark.adaptcentre.ie/ARKProjects
[7] https://gdpr.eu/

The ARK Platform incorporates incident response (IR) evaluation into its security modules to prevent cyberattacks and minimize disruption. IR teams [13], are responsible for reducing breach impacts and quickly restoring operations. While some methods aim to automate IR [14–16], existing cybersecurity ontologies focus mainly on incidents rather than the broader socio-technical context. The ARK Platform uses Semantic Web technologies to model IR processes, roles, and artifacts, defining a cybersecurity ontology and taxonomy aligned with security standards like ISO and NIST.

This work presents two security models for the ARK Platform to process sensitive data and conduct cybersecurity evaluations in socio-technical risk management. It explores the feasibility of using Semantic Web technologies to handle sensitive data and assesses how well Semantic Web standards meet the needs of a cybersecurity risk management system.

The rest of this work is organized as follows: Section 2 reviews related security approaches, Section 3 provides an overview of the ARK Platform, Section 4 details the security models using Semantic Web technologies, Section 5 discusses the implementation of these models on the ARK Platform, and Section 6 presents the conclusions.

2. SEMANTIC WEB SECURITY APPROACHES

This section examines two key security activities: the sharing of sensitive data and the implementation of cybersecurity mechanisms using Semantic Web technologies.

2.1 Sharing Sensitive Data

The mechanisms for sharing data on the web should be based on a trust-secure process that guarantees that sensitive data will be appropriately stored and processed for the actions approved by the data owner [17].

As data sharing becomes crucial in healthcare, finance, and research, adopting dataspaces is essential for ensuring trust and compliance with regulations like GDPR and HIPAA [18]. Dataspaces integrates diverse data sources while ensuring privacy and security through controlled access, anonymization, and encryption [19, 20]. They provide secure communication and features like access control, user roles, and data usage control [18–21], as well as supporting data fusion, real-time sharing, and privacy protection [18, 21, 22]. However, they lack mechanisms for GDPR-compliant personal data handling, privacy-aware logging, and secure interlinking with external resources.

In the healthcare domain, several approaches to sharing sensitive data exist. Beyan et al.[10], introduce the Personal Health Train (PHT), a distributed infrastructure that keeps healthcare data at its source, allowing data owners to retain control while using an ontology-based access control strategy. Khurshid et al.[17], present the Data Request Management System (DRMS), which manages data access for quality improvement and research. DRMS involves three phases: (i) data access, (ii) linking data from multiple sources, and (iii) clinical decision support. Linked data in phase two ensures access control based on privacy policies.

The ARK Platform consists of different modules and requires a solution for handling sensitive information that fits its architecture. While the aforementioned approaches could be adapted, a more distributed solution is needed. Thus, using dataspaces to manage sensitive data is proposed for the ARK Platform, based on Linked Data vocabularies such as DPV for personal data, the Data Catalog Vocabulary[8] (DCAT) for interlinking external resources, and PROV[9] for user logs.

2.2 Cybersecurity

Semantic Web technologies in cybersecurity aim to identify and represent system vulnerabilities by describing resources linked to contextual information [23], and cybersecurity concepts [24], to monitor and infer vulnerabilities.

Coppolino et al. [23], develop a cybersecurity system for monitoring smart grids, using Semantic Web technologies to gather contextual data on time, location, environment, and operational states to identify vulnerabilities. Aranovich et al. [24], introduce the TRONTO system, which uses an ontology of vulnerabilities to extract vulnerability-related information from social media, leveraging OWL reasoning to infer critical vulnerabilities from the National Vulnerability Database (NVD). Pastuszuk et al. [25], present the Dynamic Cybersecurity Ontology (DCO) for monitoring dynamic IT systems, mapping infrastructure data from cybersecurity search engines.

In incident response, Moreira et al.[26], introduce the Computer Security Incident Handling Ontology (CSIHO), an OWL-based framework for managing cybersecurity incidents in collaborative defense groups. Posea et al.[27], present an ontology to manage cyber incidents across Europe, connecting various cybersecurity taxonomies to improve incident reporting and tracking. Pandit et al. [28], develop a terminology for personal data processing under GDPR, which has since expanded to include aspects of cybersecurity incidents such as data breaches, risks, and controls.

The approaches described are domain-specific solutions for monitoring and inferring vulnerabilities, often using ontologies for various cybersecurity aspects. In contrast, the ARK Platform focuses on solutions based on established standards, building its cybersecurity ontology on the ISO 27000 series and NIST guidelines to represent key cybersecurity concepts.

3. THE ARK PLATFORM STRUCTURE OVERVIEW

The ARK Platform uses Semantic Web technologies to integrate and classify risk data from qualitative and quantitative sources into a unified knowledge graph. This is modeled using the ARK Cube Ontology and the ARK Platform Vocabulary. The Cube Ontology supports data analysis through the Cube methodology for managing socio-technical risks [29, 30], while the Platform Vocabulary models users, access controls, permissions, and data classifications.

The risk model, or knowledge graph, is based on the ARK CUBE Ontology, which stores CUBE questionnaire data, structures risk analyses, and organizes them into projects and stages. The ARK Platform Vocabulary models platform users, access controls, and permissions, and incorporates a

[8] https://www.w3.org/TR/vocab-dcat-2/
[9] https://www.w3.org/TR/prov-o/

data classification system aligned with the Health Service Executive (HSE) Information Classification and Handling Policy[10]. Developed by organizational psychologists and knowledge engineers using the Web Ontology Language (OWL) specification in the Protégé environment[11], both ontologies follow Gruber's guidelines for knowledge sharing, reusability, and interoperability [31]. They are consistent, extensible, and include human-readable metadata and documentation.

The ARK taxonomies were defined using the Simple Knowledge Organisation System[12] (SKOS), a W3C recommendation for expressing knowledge organisation systems. The concepts in the ARK Risk Terminology and in the HAdvInCats Terminology were defined by safety experts. The ARK Health concepts were taken from HSE Integrated Risk Management Policies[13], the HSE Incident Management Framework[14], and the HIQA National Standards for the Prevention and Control of Healthcare-Associated Infections[15]. The taxonomies can be used to annotate data entered on the platform with the view that these annotations could be used to facilitate information searches and evidence linking.

The ARK Application is built on open-source Jena knowledge base technology and uses a modern Node.js web front end to enable users to interact with ARK. From a user's perspective, the platform consists of four main components: (i) The **Risk Register** allows users to record and group risks using the HSE's risk assessment format; (ii) The **Project Analysis** component enables users to create and analyze risk management projects, linking supporting evidence to the process. This evidence is stored in ARK Evidence, a data management system built with CKAN[16]. Datasets in ARK Evidence are described using the Data Catalogue Vocabulary (DCAT) [32], ensuring interoperability with the ARK Platform; (iii) The **CUBE Analysis** component guides users through completing the CUBE questionnaires, and; (iv) the **CUBE Summary** component provides a visual overview of the Project and CUBE analyses.

The ARK Platform was designed to be extensible or customised, coping with the requirements of a particular domain or problem. The following list provides the extensions or customizations available to the ARK Platform:

- Natural language fields. Analysts can describe their domain understanding rather than limiting responses to highly structured data.
- Linking evidence to analysis. Any HTTP resource could be linked to the analysis and available for querying and reporting.
- New taxonomies. Add new taxonomies to the queryable knowledge graph of ARK, making it available to users through the user interface.

[10] https://www.hse.ie/
[11] https://protege.stanford.edu/
[12] https://www.w3.org/TR/skos-reference/
[13] https://www.hse.ie/eng/about/qavd/riskmanagement/risk-management-documentation/hse%20integrated%20risk%20management%20policy%202017.pdf.
[14] https://www.hse.ie/eng/about/qavd/incident-management/hse-2020-incident-management-framework-guidance.pdf.
[15] https://www.hiqa.ie/sites/default/files/2017-01/Safer-Better-Healthcare-Standards.pdf.
[16] CKAN-Retrievedfromhttps://ckan.org/.AccessedJuly10th,2024

- Customisable risk model and forms. The ARK risk model can be configured to different numbers of levels, impact types or likelihood definitions and thresholds. The risk forms can also be configured to use different fields or structures.
- Extension of CUBE with domain-specific questions. Adding tailored questions according to the specific domain or problem.

The following sections explore the ARK Platform's extension capabilities by integrating new security mechanisms for processing sensitive data and evaluating IR capabilities.

4. THE ARK PLATFORM SECURITY MODELS

This section discusses the implementation of two security models on the ARK Platform. Initially, the platform used access control based on authentication for access management, but lacked flexibility in securing specific information. To address this, a sensitive data processing method was introduced. Additionally, the platform was extended to evaluate IR cybersecurity issues and integrate them into the CUBE methodology.

4.1 Sensitive Data Processing

The ARK Platform addresses GDPR and ISO 27001 requirements for securely processing sensitive data. This includes personal data (PII), special categories under GDPR [17], and confidential business data that does not normally leave an organization. The Trusted Integrated Knowledge Dataspace (TIKD) [11] enables secure sharing of sensitive data within dataspaces[18].

TIKD (see FIGURE 1) uses Semantic Web technologies and trusted data-sharing mechanisms to support integrated knowledge graphs in sensitive environments. It enhances dataspace security by addressing personal data handling, data privileges, pseudonymization of user activity logs, and privacy-aware data interlinking.

The ARK Platform prioritizes security, focusing on data interlinking, privacy-aware accessibility, and secure Linked Open Data publication. It uses TIKD to manage personal, pseudonymized (GDPR-compliant), and security log data, with sensitive data processing described through DPV for GDPR compliance.

The ARK Platform collects users' personal data through a registration process to enable access to the ARK Platform. The registration requires a username, e-mail address, organization role, platform role and a password. On the other hand, the TIKD security control service authenticates an ARK user through their username or e-mail address and their password.

[17] GDPR Art.9-1
[18] A dataspace integrates and shares data from diverse sources, formats, and domains [37].

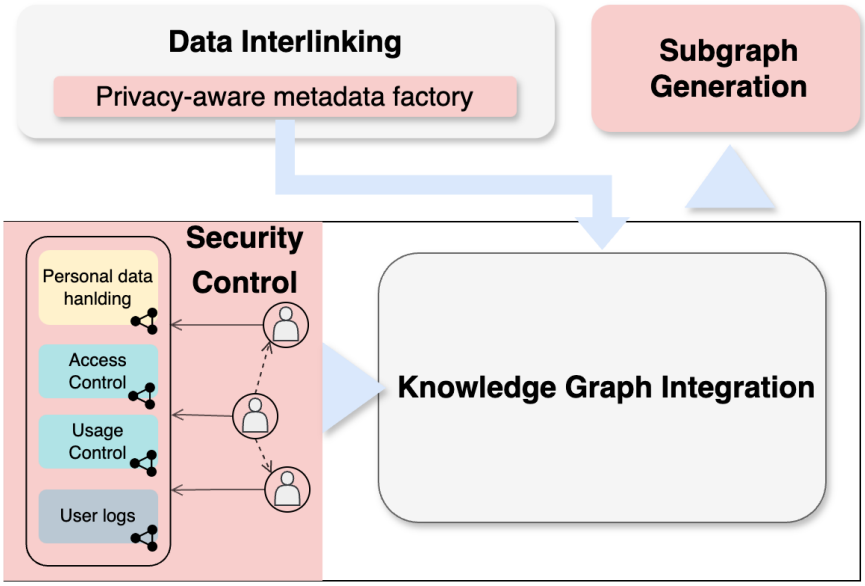

Figure 1: The Trusted Integrated Knowledge Dataspace Services.

4.1.1 Evaluation

The security assessment of the ARK Platform is based on the criteria outlined in the ISO 27001 standard. The evaluation process was conducted using the ISO 27001 Gap Analysis Tool (GAT)[19], a self-assessment questionnaire that addresses the requirements from Clauses 4 to 10 of ISO/IEC 27001:2022 and 93 controls from Annex A. The GAT consists of 41 questions organized into seven clauses, each subdivided into sub-clauses containing one or more requirements (questions). This questionnaire serves to identify gaps in compliance when implementing the ISO 27001 standards.

The evaluation process, utilizing the GAT questionnaire, was carried out both prior to and following the implementation of TIKD. Before TIKD was integrated, the ARK Platform achieved a 53.66% compliance rate. After TIKD was implemented, compliance increased to 85.37%, reflecting a significant improvement of 31.71%. However, certain requirements related to the "Context of the Organization", "Operation", "Performance Evaluation", and "Improvement" clauses still require attention in order to further enhance compliance with the ISO 27001 standard.

4.2 The Cybersecurity Ontology and Taxonomy

Incident Response (IR) is vital for preventing cyberattacks and minimizing business disruption. Galadima et al. [33] enhanced the ARK Platform by adding cybersecurity evaluation capabilities to improve incident knowledge across the IR socio-technical domain. They identified key requirements for conducting a Socio-technical Systems Analysis (STSA) of cybersecurity IR organizations, which include IR system modeling (incident data, processes, teams, CSIRT[20] organization, standards,

[19] `https://www.itgovernance.eu/en-ie/shop/product/iso-27001-gap-analysis-tool`
[20] Computer Security Incident Response Team

machine readability, and openness) and STSA requirements (model, analyst questions, coverage of STSA dimensions, Realist analysis, links to risk and safety improvement). As a result, the CUBE questionnaire was extended with specialized IR questions, and an ontology (ARK Controls Ontology) and terminology (ARK Cybersecurity Terminology) based on ISO 27000 standards were published to model IR artifacts, processes, and roles.

The ARK Cybersecurity Terminology[21] (ACT) uses the SKOS vocabulary to define and describe 140 concepts taken from ISO and NIST standards. On the other hand, the ARK Controls Ontology[22] (ACO) was developed based on the OWL 2 to define the sets of control classes and their hierarchies, taken from the ISO 27002 standard and the HSE documents, that are used on the ARK Platform. The ACO and ACT follow the NeOn methodology to develop the corresponding ontology and taxonomy.

The ACO is a unified control model encompassing various security frameworks, including ISO 27000, DPV controls, Enterprise Risk Management (ERM) concepts, and NIOSH controls[23]. It models specific controls deployed in the ARK Platform, such as password-based access control. The ACO introduces the concept of a "control group[24]," which allows controls to be organized hierarchically by themes, organizational units, or individuals, simplifying control template management. The ARK Platform also specifies control metadata, such as owners and status, to manage control lifecycles linked to risks and ARK projects.

4.2.1 Evaluation

The cybersecurity ontology and taxonomy were evaluated through the F-UJI FAIRness assessment tool [34] and the Oops! Ontology Pitfall Scanner [35] quality assessment tool.

F-UJI processes online datasets using various metrics to evaluate the 17 'FAIR Guiding Principles for scientific data management [36], focusing on the Findable, Accessible, Interoperable, and Reusable (FAIR) aspects. **Findable** data should be accessible with unique identifiers and descriptive metadata. **Accessible** data should be retrievable with persistent identifiers, even if the data is no longer available. **Interoperable** data should follow common standards, enabling integration with other sources. **Reusable** data should have clear descriptions, usage licenses, and community-endorsed formats to facilitate understanding and reuse.

F-UJI assesses compliance with the FAIR principles using four maturity levels: Incomplete, Initial, Moderate, and Advanced. These levels reflect how well a dataset meets the Findable, Accessible, Interoperable, and Reusable criteria, with "Incomplete" indicating low adherence and "Advanced" signifying high compliance. The ranges help evaluate and communicate the FAIRness of datasets. According to the results reported in [33], The ACT was scored as "Initial" and ACO as "Moderate´´.

The Oops! tool identifies 40 pitfalls, categorized as "critical", "important", or "minor". These are assessed using metrics like the Weighted Sum, Lexicographic Order, and Centroid Function. The Weighted Sum assigns weights to criteria and sums them for a final score. The Lexicographic

[21] https://openark.adaptcentre.ie/Ontologies/ARKControlTerminology/index-en.html
[22] https://openark.adaptcentre.ie/Ontologies/ARKControlOntology/index-en.html
[23] https://www.cdc.gov/niosh/hierarchy-of-controls/about/index.html
[24] https://openark.adaptcentre.ie/Ontologies/ARKControlOntology/index-en.html#ControlGroup

Order ranks ontologies by severity, prioritizing the most critical. The Centroid Function calculates intervals for each severity level, offering an alternative ranking approach.

These metrics are used to evaluate the effectiveness of the ranking method, with the Kendall coefficient computed to measure similarity between rankings. Based on findings in [33], no critical pitfalls were found, but common issues included ”untyped class[25]” and “missing disjointness[26]”. A common minor pitfall was “merging different concepts into the same class[27]”.

5. DISCUSSION

The security models discussed demonstrate the effectiveness of using Semantic Web technologies for security frameworks. TIKD uses DPV to describe PII, ensuring GDPR compliance, and offers a security solution based on dataspaces and Semantic Web standards like PROV-O, DCAT, and SKOS. The ARK Platform enhances its security alignment by integrating these elements, with the Gap Analysis Tool for ISO 27001 showing an improvement in compliance from 53.66% to 85%. This highlights the value of Semantic Web technologies in meeting stringent security standards.

The ARK Platform’s extension to evaluate IR in socio-technical systems showcases the use of Semantic Web technologies to address diverse domain requirements through linked data principles. ACO and ACT were developed based on various standards and security controls, with future extensibility in mind. The Semantic Web’s goal of providing reusable resources is reflected in ACO and ACT, which focus on describing resources using standards and security documents, rather than specific requirements.

Implementing these models is challenging due to the need for coordination between system modules and expertise in query languages to integrate security logic. A drawback of using Semantic Web technologies for security modules is the impact of vocabulary updates or changes, which can affect system logic, predefined queries, and the knowledge base.

6. CONCLUSION

The ARK Platform demonstrates how Semantic Web technologies can effectively address the challenges of cybersecurity and sensitive data management in socio-technical risk environments. By integrating TIKD for secure data processing and developing the ARK Controls Ontology (ACO) and Cybersecurity Taxonomy (ACT), the platform achieves compliance with standards like ISO 27001 and GDPR. These security models not only enhance sensitive data processing through privacy-preserving mechanisms but also extend the platform’s capabilities to evaluate incident response in cybersecurity. The substantial improvement in compliance rates and the integration of FAIR principles underscore the platform’s robustness and adaptability for real-world applications.

[25] refers to a class within an ontology that has not been assigned a specific type or category
[26] refers to the absence of explicit definitions of disjoint relationships between classes or properties
[27] refers to using a single class for multiple distinct concepts that should be separate.

The Semantic Web-based approach facilitates modularity and extensibility, allowing organizations to tailor the ARK Platform to their specific operational requirements. Through ACO and ACT, the platform connects risk management with standardized cybersecurity frameworks, enabling effective analysis and reporting. However, the study also highlights some challenges, such as the need for specialized expertise in ontology development and the potential disruption caused by vocabulary updates. Despite these limitations, the ARK Platform provides a scalable solution for integrating cybersecurity into broader risk governance frameworks.

Future work will extend the ARK Controls Ontology and the ARK Platform to support management capabilities for security controls in an organization. This will include new properties and concepts to support verification of controls at the operational level and controls assurance at the strategic organizational level. Our work will be based on linking the concepts of controls attestation with the obligation to act from the Cube framework. For example, for verification it will describe the state and life-cycle of a control, e.g. to identify effective, partially effective and ineffective controls, link that assessment with evidence and the identity of a verifier for accountability.

References

[1] Berners-Lee T, Hendler J. Publishing On The Semantic Web.. Nature. 2001;410:1023-1024.

[2] Bizer C, Heath T, Idehen K, Berners-Lee T. Linked Data on the Web (LDOW2008). In: Proceedings of the 17th international conference on world wide web. 2008:1265-1266.

[3] Bernasconi E, Ceriani M, Di Pierro DD, Ferilli S, Redavid D. Linked Data Interfaces: A Survey. Information. 2023;14:483.

[4] Kalos V, Polyzos GC. Requirements and Secure Serialization for Selective Disclosure Verifiable Credentials. In: IFIP International Conference on ICT Systems Security and Privacy Protection. Springer. 2022:231-247.

[5] Lee J, Choi J, Oh H, Kim J. Privacy-Preserving Identity Management System. Cryptol Eprint Arch. 2021.

[6] Garcia K, Zihlmann Z, Mayer S, Tamo-Larrieux A, Hooss J. Towards Privacy-Friendly Smart Products. In: 18th International Conference on Privacy Security and Trust (PST). IEEE. 2021:1-7.

[7] Hickey D, Brennan R. A GDPR International Transfer Compliance Framework Based on an Extended Data Privacy Vocabulary (DPV). In: Legal knowledge and information systems. IOS Press. 2021:161-170.

[8] Ryan P, Brennan R. Demonstrating GDPR Accountability With Csm-Ropa: Extensions to the Data Privacy Vocabulary. In: ICEIS. SCITEPRESS - Science and Technology Publications. 2021:591-600.

[9] Crotti Junior A, Basereh M, Abgaz Y, Liang J, Duda N, et. al. The Ark Platform: Enabling Risk Management Through Semantic Web Technologies. In: Proceedings of the 11th international conference on biomedical ontologies (ICBO) Italy. 2020:1-10.

[10] Beyan O, Choudhury A, Van Soest J, Kohlbacher O, Zimmermann L, et. al. Distributed Analytics On Sensitive Medical Data: The Personal Health Train. Data Intellegence. 2020;2:96-107.

[11] Hernandez J, McKenna L, Brennan R. TIKD: A Trusted Integrated Knowledge Dataspace for Sensitive Data Sharing and Collaboration. In Data Spaces: Design Deployment and Future Directions. Cham: Springer International Publishing. 2022:265-291.

[12] Sovrano F, Vitali F, Palmirani M. Modelling Gdpr-Compliant Explanations for Trustworthy AI. In: Electronic Government and the Information Systems. Perspective: 9th International Conference EGOVIS Bratislava Slovakia Proceedings. 2020;9:219-233.

[13] Steinke J, Bolunmez B, Fletcher L, Wang V, Tomassetti AJ, et al. Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research. IEEE Secur Privacy. 2015;13:20-29.

[14] Ahmad A, Desouza KC, Maynard SB, Naseer H, Baskerville RL. How Integration of Cyber Security Management and Incident Response Enables Organizational Learning. J Assoc Inf Sci Technol. 2020;71:939-953.

[15] Ahmad A, Maynard SB, Desouza KC, Kotsias J, Whitty MT, et. al. How Can Organizations Develop Situation Awareness for Incident Response: A Case Study of Management Practice. Comput Sec. 2021;101:102122.

[16] He Y, Zamani ED, Lloyd S, Luo C. Agile Incident Response (Air): Improving the Incident Response Process in Healthcare. Int J Inf Manag. 2022;62:102435.

[17] Khurshid A, Rousseau JF, Andrews SB, Tierney WM. Establishing a Data-Sharing Environment for a 21st-Century Academic Health Center. ACI Open. 2020;4:e59-68.

[18] Curry E, Derguech W, Hasan S, Kouroupetroglou C, ul Hassan U. A Real-Time Linked Dataspace for the Internet of Things: Enabling “Pay-As-You-Go” Data Management in Smart Environments. Future Gener Comput Syst. 2019;90:405-22.

[19] Munoz-Arcentales A, López-Pernas S, Pozo A, Alonso Á, Salvachúa J, et. al. An Architecture for Providing Data Usage and Access Control in Data Sharing Ecosystems. Procedia Comput Sci. 2019;160:590-597.

[20] Otto B, Hompel M, Wrobel, S. International Data Spaces. Berlin Heidelberg: Springer Berlin Heidelberg. 2019:109-28.

[21] Wei S, Zhihua H, Zikai W, Zheng Y, Wei D. A Method and Application for Constructing a Authentic Data Space. In: IEEE International Conference on Internet of Things and Intelligence System IoTaIS Bali Indonesia IEEE. 2019:218-224.

[22] Sun Y, Yin L, Sun Z, Tian Z, Du X. An Iot Data Sharing Privacy Preserving Scheme. In: 39th IEEE Conference on Computer Communications INFOCOM Workshops Toronto ON Canada. IEEE. 2020:984-990.

[23] Coppolino L, Nardone R, Petruolo A, Romano L, Souvent A. Exploiting Digital Twin Technology for Cybersecurity Monitoring in Smart Grids. In: Proceedings of the 18th international conference on availability reliability and security. New York USA: ACM. 2023:1-10.

[24] Aranovich R, Wu M, Yu D, Katsy K, Ahmadnia B, et. al. Beyond NVD: Cybersecurity Meets the Semantic Web. In: Proceedings of the 2021 New security paradigms workshop. New York USA: ACM. 2021:59-69.

[25] Pastuszuk J, Burek P and Książopolski B. Cybersecurity Ontology for Dynamic Analysis of IT Systems. Procedia Computer Science 2021;192:1011–1020.

[26] Moreira GB, Calegario VM, Duarte JC, Dos Santos AF. Csiho: An Ontology for Computer Security Incident Handling. In: Anais do XVIII simpósio brasileiro de segurança da informação e de sistemas Computacionais. Sociedade Brasileira de Computação – SBC. 2018:1-14.

[27] Posea V, Sharkov G, Baumann A, and Chatzichristos G. Towards unified European cyber incident and crisis management ontology. Information & Security 2022;53:33-44.

[28] Pandit HJ, Polleres A, Bos B, Brennan R, Bruegger B, et. al. Creating a Vocabulary for Data Privacy: The First-Year Report of Data Privacy Vocabularies and Controls Community Group (DPVCG). On the move to meaningful Internet systems: OTM conferences: confederated international conferences: CoopIS ODBASE C&TC Rhodes Greece. Proceedings. In: Springer. 2019:714-30.

[29] Corrigan S, Kay A, O'Byrne K, Slattery D, Sheehan S, et. al. A Socio-Technical Exploration for Reducing & Mitigating the Risk of Retained Foreign Objects. Int J Environ Res Public Health. 2018;15:714.

[30] McDonald N. The Evaluation of Change. Cogn Tech Work. May 2015;17:193-206.

[31] Gruber TR. Toward Principles for the Design of Ontologies Used for Knowledge Sharing? Int J Hum Comput Stud. 1995;43:907-928.

[32] Albertoni R, Browning D, Cox S, Gonzalez-Beltran AN, Perego A, et. al. The W3C Data Catalog Vocabulary. version 2 Rationale design principles and uptake. Data Intelligence. 2023:1-37. 2024;6:457-487.

[33] Galadima HS, Doherty C, McDonald N, Liang J, Brennan R. Evaluating Incident Response in Csirts Using Cube Socio-Technical Systems Analysis. Available at SSRN 4854628. Computer Standards & Interfaces. 2025;93:103970.

[34] Devaraju A, Huber R. F-Uji – An Automated Fair Data Assessment Tool. 2024.

[35] Poveda-Villalón M, Gómez-Pérez A, Suárez-Figueroa MC. Oops! (Ontology Pitfall Scanner!). Int J Semant Web Inf Syst. 2014;10:7-34.

[36] Wilkinson MD, Dumontier M, Aalbersberg IJ, Appleton G, Axton M, et. al. The Fair Guiding Principles for Scientific Data Management and Stewardship. Sci Data. 2016;3:160018. 2016;3:1-9.

[37] Atzori M, Ciaramella A, Diamantini C, Martino B, Distefano S, et. al. Dataspaces: Concepts Architectures and Initiatives. In: CEUR WORKSHOP proceedings. CEUR-WS. 2024;3606.