Using Knowledge Graphs to ensure Privacy Policies in decentralized data collection systems

Biagio Boi
University of Salerno
Fisciano, Salerno, Italy
bboi@unisa.it

Christian Esposito
University of Salerno
Fisciano, Salerno, Italy
esposito@unisa.it

ABSTRACT

As data collection systems become more complex and pervasive, ensuring transparency and accountability in the acquisition and use of personal data becomes increasingly critical. This work investigates the use of knowledge graphs as a solution to this problem, emphasizing their capacity to represent and enforce privacy laws in a decentralized setting. Knowledge graphs provide full privacy management and can be applied also to decentralized systems by providing a consistent representation of data and privacy policies. We specifically discuss how knowledge graphs can be used to track consent management and data retention policies; we also present a case study of our framework in action, demonstrating how it can be used to ensure transparency in an increasingly popular decentralized data collection system. The implementation of such a framework in a decentralized context shows that the use of knowledge graphs can provide a transparent and accountable view of the data collection process, improving trust and confidence in the system among both data subjects and regulators.

CCS CONCEPTS

• **Security and privacy → Privacy-preserving protocols**; **Digital rights management**; **Access control**.

KEYWORDS

Knowledge Graphs, Privacy, Decentralization

ACM Reference Format:
Biagio Boi and Christian Esposito. 2023. Using Knowledge Graphs to ensure Privacy Policies in decentralized data collection systems. In *International Conference on Research in Adaptive and Convergent Systems (RACS '23), August 6–10, 2023, Gdansk, Poland.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3599957.3606213

1 INTRODUCTION

Thanks to the introduction of smart devices and the progress in terms of connectivity, cities are always more interconnected offering valuable services to the citizens that use them for improving their life. Devices collect valuable data and process them in order to provide them as input to Machine Learning (ML) models, which are able to handle route optimization, parking, street lights, accident prevention/detection, and other services. An increasing number of cities leverage these models and data to create the so-called *smart transportation* [18], able to reduce congestion and increase the satisfaction of their citizens.

In some cases, these data also collect personal information, which may introduce a lack of privacy for citizens, increasing the risk of re-identification if a strong security mechanism is not considered in the design phase. General Data Protection Regulametation (GDPR) defines the principles to be considered when designing a system; a technique, that is usually used in big data collection context, and able to comply with GDPR is the *data anonymization* [12], which leverages randomization and generalization to decrease the linkability of information. These techniques in some cases completely remove the connection existing between data and users, making it difficult to be applied in a context where a strong connection is requested. Moreover, despite data produced by sensors in these contexts being typically anonymized, they are sometimes stored in centralized and siloed systems where access is reserved for authorized users. The disadvantages of this approach are huge, a complex database is sometimes put in place causing relationships between data to require huge power computation and interaction with tens of tables.

With the advent of blockchain and more in general of decentralization, data are moving away from centralized servers in order to increase the level of privacy. Multiple works have been done adopting different technologies, and some applications of blockchain within the medical context can be found in [16]. An emerging technology aiming at decentralizing the Internet giving the users possibility to self-host their data is characterized by Solid ecosystem [10] which leverages the concept of Knowledge Graphs (KGs) for representing data. In such a scenario needs for anonymization is in part reduced since users can decide whether share or not to share collected data. The usage of KGs [8] is simplifying the life of the data analyst thanks to a more flexible representation of data; differently from the database, in KGs, nodes represent entities while edges represent binary relations between those entities. Solid leverages ontologies also for handling with authorization adopting two mechanisms based on Access Control List (ACL) ontologies; an example is depicted in the Listing 1.

A typical user can decide which are applications (domains) authorized to perform actions on stored data. This representation is an example that demonstrates KGs are not limited to data representation but, thanks to their flexibility, can be used for the representation of multiple concepts. Another example of adoption is characterized by vulnerability [14], where an automated tool for the analysis is proposed on the basis of KGs. KGs can be used for

RACS '23, August 6–10, 2023, Gdansk, Poland

ACM ISBN 979-8-4007-0228-0/23/08…$15.00
https://doi.org/10.1145/3599957.3606213

representing both data and concepts; data querying and re-use is difficult if considering them in correlation with privacy policies. For ex., a citizen may want the municipality to collect his data on traffic but not those related to the number of times he takes the bus.

Listing 1: ACL policies defined by Solid

```
@prefix acl: <http://www.w3.org/ns/auth/acl#>.

:me
   acl:trustedApp
         [
            acl:mode acl:Append, acl:Control, acl:
                ↪ Read, acl:Write;
            acl:origin <https://unisa.it>
         ].
```

In this paper, we will explore the key components and methodologies involved in integrating KGs into privacy policy representation. We will discuss the challenges and opportunities in developing knowledge graph-based privacy management frameworks and examine existing research and practical implementations in this domain. These graphs enable fine-grained control over data access where Solid is already applying a KGs-based system. We will consider such an implementation as an enabler for our solution, demonstrating how ACL and privacy policies can be merged in order to create a unique graph. Additionally, we will address potential limitations and future directions to further improve the efficacy of privacy policies enforced through KGs. The introduction of this technology in the smart city context can be a starting point for improving data management while considering the always more increasing complexity of privacy policies. The document is structured into five sections:

- The second section discusses other works in this field, with a particular focus on the usage of KGs in the context of smart cities and privacy policies representation;
- The third section introduces the architecture and design of our system considering all the components needed for implementing a decentralized solution for privacy policies representation;
- The fourth section discusses a possible integration within the Solid ecosystem;
- In the last section conclusions and future development are discussed;

2 STATE OF THE ART

The increasing number of data-collecting applications can be a threat if privacy and security concerns are not taken into consideration during the design phase. In addition, some applications read sensible information whose consensus to the acquisition of user data must be taken into account in adherence to GDPR principles. Different research has been conducted in this context, in order to apply some techniques able to manage users' consensus in a transparent and updatable way.

KGs are a graph-based knowledge representation model that captures entities, relationships, and attributes in a structured and interconnected manner. It provides a flexible framework for organizing and representing complex knowledge, allowing for the integration of heterogeneous data from diverse sources. KGs excel at capturing the richness and complexity of real-world information and establishing meaningful connections between different pieces of data.

A study conducted by Zou [19] highlights the possible usage of KGs, among them is particularly interesting the application in a cyber security context, where detection of cyber security events can be done using the inherent knowledge reasoning ability of KG. On the same line, Yang et al. [17] leverage KGs for representing relevance between objects and image privacy creating a graph-based neural network; confirming how KGs can be used for representing abstract or concrete concepts in a really dense scenario such as the artificial intelligence one. Sharma and Bhatt [15] investigate the usage of KGs within the context of healthcare applications as an enabler for privacy-preserving. They make a connection between disease and symptoms and between patients and symptoms in order to help the doctor to make a decision. Moreover, it anonymizes the patients' data by changing the label associated with nodes making such graphs available for ML models without restriction on privacy.

All these works can be considered as an extension of our proposal, namely something that can be built upon our solution. The main focus is to build a KG able to represent privacy policies while capturing users' data.

A starting point for the resolution of our problem has been fixed by Cui et al. [3], who propose a framework for automatically capturing privacy policy from relations between different parts of text despite the challenges coming from Natural Language Processing (NLP). Such a framework produces KGs able to represent privacy policies and their dependencies. Considering this work at the bottom of our solution can represent an automated system where policies are directly represented as KGs and users need only to accept them.

It is possible to increase the reuse of KG: ontologies provide a formal and standardized way to define concepts, relationships, and constraints within a specific domain. Web Ontology Language (OWL) [11] is the most widely known language used to describe the semantics of data and enable precise reasoning over it. Ontologies play a crucial role in enhancing data interoperability and ensuring semantic consistency across different knowledge sources. Within smart cities, multiple ontologies have been proposed during the last years, whose applications have been analyzed by De Nicola et al. [4] which highlights more than 100 works in this field, confirming how the adoption of these ontologies could be a resolution for the interoperability for a high heterogenous system such smart city one. An interesting ontology, encoded in OWL, for the representation of privacy policies, has been proposed by Fernandez et al. [7].

The combination of KGs and ontologies offers a powerful approach to organizing, representing, and reasoning over complex data. It enables us to harness the full potential of interconnected information, unlock hidden insights, and build intelligent systems that can reason and understand the world in a more sophisticated way. Despite all these approaches being interesting from a different perspectives, poor work has been done in trying to combine data and privacy policies using a well-defined ontology into data decentralization approaches such as Solid. In the next section, a design of our proposal is introduced by considering the research already conducted in this context.

3 DESIGN

The main difference between databases and KGs is the flexibility while considering strong structure organization based on ontologies. In a KG it is still possible to represent a relationship between entities simply by drawing an edge between nodes. The major novelty introduced by our study is the possibility to integrate privacy policy in a system that collects data. In this way, applications are allowed to collect all data from users depending on the authorization that users to the requested policies. Analogously, those who want to read data are able to read only what the users choose to make it possible to read adopting privacy policies that can be a kind of classification in reading data. In what follows we will explain the major components of our system, with a particular focus on the graph representation and possible interactions with such defined graphs. One of the major standards in this field for generating graphs is the Resource Description Framework (RDF) which will be taken into consideration in the design of our proposal. Moreover, Turtle and SPARQL offer simple language for encoding and querying an RDF graph respectively.

The approach defined below can be applied to traditional KGs, but it is not enough for handling privacy issues. In the next section, we will explain how to decentralize these graphs by leveraging on Solid ecosystem.

3.1 Graph Construction

In RDF, each thing is described as a resource that is identified by a Uniform Resource Identifier (URI). Resources must be able to represent all the concepts and parties of our system; in particular, a resource can be the representation of:

(1) **Users**, namely the passive users of the system, which are the target of the application interested in collecting data related to the user. Each user has his own properties related to his information such as name, surname, date of birth, and so on;
(2) **Applications**, which are responsible for collecting data. Each application has its own properties;
(3) **Privacy Policies**, created staring from textual representation using method defined in [3];

The flexibility of KGs makes it possible to consider other resources as extensions of these three described: an example could be the existence of smart devices connected to Applications to represent which are the sensors used. Moreover, changes in data structure and in policies can be taken into consideration by drawing new nodes; in the following section, we will consider an example that includes data generated by the application as an extension of defined nodes.

3.2 Information Representation

The power of a KG is the possibility to represent concepts and data using expressions more oriented to the human language rather than the computational one. The base unit for information representation in RDF is the statement, which is a triple constituted by: *subject*, *predicate*, and *object*.

A *subject* is one of the system resources, in our case one among Users, Applications, or Privacy Policies. A *predicate* is the property of a subject, while the *object* is the value given to the statement, which can also be referring to another resource. In particular, an *object* refer to another resource each time one of the following action happens:

(1) Users to Applications - whenever a user accepts the data collection related to an application;
(2) Applications to Privacy Policies - whenever an application needs for given policies;
(3) Users to Privacy Policies - whenever the user accepts the policies;

Some examples can be done by referring to the statement in the form of <Subject><Predicate><Object> and are depicted in Figure 1:

- <user1><citizenOf><Salerno>
- <user1><hasSex><Male>
- <user1><acceptsPolicy><policy1>
- <trustedApp><appliestTo><policy1>
- <data1><generatedBy><trustedApp>
- <data1><belongToUser><user1>

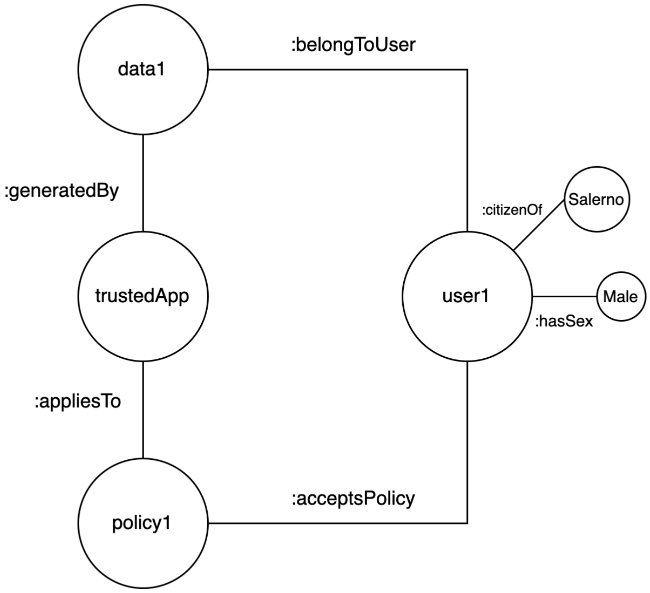

Figure 1: An example of Knowledge Graph including privacy policies

As it is possible to see some of them are referred to as Literal, which is the case of user1 in association with *Salerno* and *Male*; while the others are connected to other resources. In order to simplify the diagram, the URI has been truncated and simplified but in a realistic scenario, each node is labeled with a URI. The extended version of this graph can include multiple applications which generate huge data related to different users. In the case of the adoption of this graph in a decentralized context, as we will explain in the next section, the graph is truncated to store only data that belongs to the related user.

3.3 Encoding

In order to create a graph able to comply with querying is necessary to express RDF data in a syntax that can be reusable at the time of the querying process; one of the major query languages in this context. Turtle ("Terse RDF Triple Language") is able to comply with described requirements leveraging on the triple defined from the RDF structure. Since Turtle is able to serialize only valid graphs, it is also a useful validator.

It is possible to consider again the statements described in Figure 1 and extend it including data coming from sensors. In Listing 2 a complete example of a smart city that adopts a KG for the representation of produced data and privacy policies is given.

Listing 2: A complete Turtle Representation

```
@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-
    ↪ ns#> .
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#>
    ↪  .
@prefix xsd: <http://www.w3.org/2001/XMLSchema#> .
@prefix smartcity: <#> .
@prefix app: <#applications/> .
@prefix user: <#users/> .
@prefix sensor: <#sensors/> .

# Privacy Policies
smartcity:policy1 rdf:type smartcity:PrivacyPolicy ;
    rdfs:label "Policy 1" ;
    smartcity:appliesTo app:trustedApp .

# Applications
app:trustedApp rdf:type smartcity:Application ;
    rdfs:label "trustedApp" .

# Users
user:user1 rdf:type smartcity:User ;
    rdfs:label "User 1" ;
    smartcity:acceptsPolicy smartcity:policy1 .

# Sensor Data
sensor:data1 rdf:type smartcity:SensorData ;
    smartcity:generatedBy app:trustedApp ;
    smartcity:recordedAt "2023-05-18T10:00:00"^^xsd:
        ↪ dateTime ;
    smartcity:hasValue "25.4" ;
    smartcity:belongsToUser user:user1 .
```

The Turtle representation of statements can be easily done by referring to prefixes, notice that the properties defined can be easily extended to include more details on policies and increase the granularity of acceptance.

Web Ontology Language (OWL) can be applied to extend the meaning of the RDF graph; it defines the structure and advanced relationship between data. Moreover, they can be used for making data more interoperable between different systems and for automation tasks.

3.4 Querying

In a traditional database-based system, the interrogation of the data can be done by adopting a simple query. Nothing changed with the adoption of KGs, it is still possible to manipulate data in KG using a query-based approach. A popular language in this context is SPARQL, which is able to interact with KGs using a syntax similar to SQL.

Listing 3 depicts a query as a simple interaction with the KG, which request which is the user who accepted a given privacy policy.

Listing 3: Retrieve users applying to a policy using SPARQL

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-
    ↪ ns#>
PREFIX smartcity: <http://example.com/smartcity#>

SELECT ?user
WHERE {
  ?user rdf:type smartcity:User ;
        smartcity:acceptsPolicy smartcity:policy1 .
}
```

3.5 Discussion

The structure of KGs for representing privacy policies has been described, it is a simple extension of a traditional KG where nodes are the policies and edges are the acceptance or rejection of these policies. Leveraging them is possible to describe all the policies requested from an application and a user is able to accept only a part of them. The adoption of them in a high-density context, where myriads of devices are connected to an increasing number of applications and policies can be a simplification for municipalities as well as citizens. A challenge lies in the interoperability and standardization of KGs across different platforms and entities. In order to achieve seamless integration and effective privacy enforcement, there is a need for common data models, ontologies, and standards for representing privacy policies within KGs. Standardization efforts should be encouraged to promote interoperability and enable the exchange of privacy-related information across decentralized systems. To make privacy policies more human-readable it is possible to build something upon the KGs. JSON-LD (Linked Data) offers a compact representation of linked information, which could be leveraged in this context for increase the potential of this privacy management system. When considering a KG for handling privacy policies, JSON-LD can play a significant role in structuring and representing the data within the graph, not only in the creation phase but also during the evolution of applications.

One of the major principles of GDPR regards the need of taking humans in the loop in an automated system: JSON-LD can guarantee this by creating connections between the data represented. It is possible to use the *linkability* of this technology for informing users of changes that could happen in policies during their evolution. Moreover, it is possible to create a direct association between requests done and defined policies - an application could be able to perform actions on data referring to policies and logging the usage of that policies so that the user can be informed of the operations done on data.

4 SOLID IMPLEMENTATION

An interesting application of the given design can be found in the Solid ecosystem. As introduced in the previous section, in order to protect users' privacy we need to implement some mechanism for decentralizing the way in which these graphs are stored (ex. we want to store application data away from a centralized server). Solid aims at decentralizing the way in which data produced are stored; which can be a perfect use case for our proposal. When KGs are distributed among nodes take the name of Distributed Knowledge Graphs (DKGs), that is what Solid implements.

4.1 Data Storage

Solid leverages DKGs for representing policy rules as described in the Listing 1 by defining which are the permission for each application, enabling in this way a fine-grained access control. Such relationships are stored in a decentralized and user-centric manner in a space owned by the users, namely a Solid Pod. The concept of Solid Pod is to give back to the user the data ownership without storing on any server these data. In our use case, described in the previous section and represented by Listing 2, Solid can be directly applied in order to decentralize sensor data produced by applications. Using Solid in the context of privacy policies make them easily implementable in a decentralized way, where the users are the owner of the data produced by smart city sensors together with acceptance policies.

4.2 Users Notification

The motivations for using Solid as an implementation means are not limited to the decentralization offered by this ecosystem but also to the mechanisms for handling notifications. Braun and Kaefer [1] proposed support in Solid for Web Push Notifications; namely, the users are able to receive notifications even when the app is closed. In such a way, privacy changes can be notified instantly to the users that can revoke the authorizations if some radical changes happen. Notifications are an important aspect of Solid also for the access to data, where the users can be notified each time an application access data, enhancing the overall auditing.

By integrating Solid and a knowledge graph, it is possible to establish a decentralized and user-centric approach to privacy policy management, giving users more control over their data and enabling applications to make privacy-aware decisions based on the linked data.

4.3 Policy representation

It is clear that Solid leverages DKGs for handling privacy policies but some limitations still exist on their representation. In this subsection, we will analyze the mechanisms used by Solid together with a recent metadata language that can be easily built on top of our solution. Under the umbrella of the Solid project, two specifications have been considered for the representation of access control [2]: Web Access Control (WAC) and Access Control Policy (ACP).

WAC is a decentralized cross-domain access control system providing a way for Linked Data systems to set authorization conditions on HTTP resources using the ACL model. In particular, authorizations are described using ACL ontology, which leverages on knowledge graph for representing the access privileges of a requested resource.

ACP, similarly, is a language for describing, controlling, and granting access to resources; also in this case ACL ontologies are used to express such privileges of a requested resource. Following the definition of Solid protocol, a server must conform to either or both approaches.

Such solutions are limited to access control and not consent management, and it also suffers from a poor matching with the GDPR regulatory requirements, as it is not meant to express the legal bases to have a lawful treatment or neither specify access restrictions based on user preferences. To improve this, some research efforts have been conducted, where the prominent one is described in [6] using the Open Digital Rights Language (ODRL) [9] and the Data Privacy Vocabulary (DPV) [13] with the intention to have a proper representation as an ODRL profile for a GDPR-complaint access control. DPV's terms are defined using abstract semantic notions Concepts and Relations derived from Simple Knowledge Organization System (SKOS) concepts and semantic relations respectively. DPV also provides serialization in accordance with OWL making it compatible with other existing OWL-based systems. On the same line, ODRL leverages RDF classes, predicates, and named entities composing a proper Core Vocabulary.

However, there is still a lack of properly representing GDPR actors and specific access control policies to data within pods based on such roles. Referring to GDPR's Articles 13 and 14 require that entities processing personal data provide transparent information on identity, processing purpose, personal data categories, legal basis, recipients, and so on when they use personal data directly or indirectly obtained from individuals. The establishment of a metadata language for Solid (PLASMA) [5] is a promising solution to deal with these issues and have a lawful data treatment according to GDPR obligations.

Our work can be considered as a basis for describing technologies, particularly ODRL and DPV, which offer the basis for constructing a more structured system that considers a good level of granularity. Finally, considering also PLASMA which aims at solving use-cases in terms of: *What?, Who?, Where?, Why?, When? and How?* let the users be always informed about their consents and how their data are processed by applications.

5 CONCLUSION

An approach for representing data and privacy policies in KGs has been proposed considering existing work in this field. This adaptive approach is precious in environments where data undergoes transformations and flows across different platforms, as the privacy policies can be dynamically applied based on the current context. Solid offers an important starting point for the decentralization of users' data, where the managing of users' privacy policies can be done using the proposed architecture. We have planned to evaluate the proposed approach in terms of scalability and security. Policy representation is characterized by multiple challenges, where the creation of well-structured relationships starting from natural language description is a complex task. The exploration of ML and NLP in conjunction with Knowledge Graphs for privacy management is still at the beginning and has already shown the potential for enhancing the automation and efficiency of privacy policy enforcement, enabling more accurate and personalized privacy decisions. Other research can be done in order to increase the ontologies related to the policies, where a starting point for their representation has been done recently in [3] and [6]. Automation in privacy policies can be a clear starting point, always been a critical task in most applications due to the limitations imposed by GDPR.

ACKNOWLEDGEMENTS. This work was partially supported by project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NGEU.

REFERENCES

[1] Christoph H-J Braun and Tobias Käfer. 2022. Web Push Notifications from Solid Pods. In *Web Engineering: 22nd International Conference, ICWE 2022, Bari, Italy, July 5–8, 2022, Proceedings*. Springer, 487–490.

[2] S. Capadisli, Tim Berners-Lee, Ruben Verborgh, and Kjetil Kjernsmo. 2022. Solid Protocol. (2022). https://solidproject.org/TR/2022/protocol-20221231

[3] Hao Cui, Rahmadi Trimananda, Athina Markopoulou, and Scott Jordan. 2022. PoliGraph: Automated Privacy Policy Analysis using Knowledge Graphs. *arXiv preprint arXiv:2210.06746* (2022).

[4] Antonio De Nicola and Maria Luisa Villani. 2021. Smart city ontologies and their applications: a systematic literature review. *Sustainability* 13, 10 (2021), 5578.

[5] B. Esteves and H. J. Pandit. 2022. Policy Language for Solid's Metadata-based Access Control (PLASMA). (2022). https://harshp.com/plasma/

[6] Beatriz Esteves, Harshvardhan J Pandit, and Víctor Rodríguez-Doncel. 2021. ODRL profile for expressing consent through granular access control policies in solid. In *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 298–306.

[7] Javier D Fernández, Marta Sabou, Sabrina Kirrane, Elmar Kiesling, Fajar J Ekaputra, Amr Azzam, and Rigo Wenning. 2020. User consent modeling for ensuring transparency and compliance in smart cities. *Personal and Ubiquitous Computing* 24 (2020), 465–486.

[8] Aidan Hogan, Eva Blomqvist, Michael Cochez, Claudia d'Amato, Gerard de Melo, Claudio Gutierrez, Sabrina Kirrane, José Emilio Labra Gayo, Roberto Navigli, Sebastian Neumaier, et al. 2021. Knowledge graphs. *ACM Computing Surveys (CSUR)* 54, 4 (2021), 1–37.

[9] R. Iannella and S. Villata. 2018. ODRL Information Model 2.2. (2018). https://www.w3.org/TR/2018/REC-odrl-model-20180215/

[10] Essam Mansour, Andrei Vlad Sambra, Sandro Hawke, Maged Zereba, Sarven Capadisli, Abdurrahman Ghanem, Ashraf Aboulnaga, and Tim Berners-Lee. 2016. A demonstration of the solid platform for social web applications. In *Proceedings of the 25th international conference companion on world wide web*. 223–226.

[11] Deborah L McGuinness, Frank Van Harmelen, et al. 2004. OWL web ontology language overview. *W3C recommendation* 10, 10 (2004), 2004.

[12] Chunchun Ni, Li Shan Cang, Prosanta Gope, and Geyong Min. 2022. Data anonymization evaluation for big data and IoT environment. *Information Sciences* 605 (2022), 381–392.

[13] A. Polleres. 2022. Data Privacy Vocabulary (DPV). (2022). https://www.w3.org/community/reports/dpvcg/CG-FINAL-dpv-20221205/

[14] Shengzhi Qin and KP Chow. 2019. Automatic analysis and reasoning based on vulnerability knowledge graph. In *Cyberspace Data and Intelligence, and Cyber-Living, Syndrome, and Health: International 2019 Cyberspace Congress, CyberDI and CyberLife, Beijing, China, December 16–18, 2019, Proceedings, Part I 3*. Springer, 3–19.

[15] N Sharma and R Bhatt. 2022. Privacy preserving knowledge graph for healthcare applications. In *Journal of Physics: Conference Series*, Vol. 2339. IOP Publishing, 012013.

[16] Peng Xi, Xinglong Zhang, Lian Wang, Wenjuan Liu, and Shaoliang Peng. 2022. A review of Blockchain-based secure sharing of healthcare data. *Applied Sciences* 12, 15 (2022), 7912.

[17] Guang Yang, Juan Cao, Zhineng Chen, Junbo Guo, and Jintao Li. 2020. Graph-based neural networks for explainable image privacy inference. *Pattern Recognition* 105 (2020), 107360.

[18] Fotios Zantalis, Grigorios Koulouras, Sotiris Karabetsos, and Dionisis Kandris. 2019. A review of machine learning and IoT in smart transportation. *Future Internet* 11, 4 (2019), 94.

[19] Xiaohan Zou. 2020. A survey on application of knowledge graph. In *Journal of Physics: Conference Series*, Vol. 1487. IOP Publishing, 012016.