DEÜ FMD 25(74), 417-432, 2023

Dokuz Eylül Üniversitesi Mühendislik Fakültesi Fen ve Mühendislik Dergisi
Dokuz Eylul University Faculty of Engineering Journal of Science and Engineering

Basılı/Printed ISSN: 1302-9304. Elektronik/Online ISSN: 2547-958X

Ontology Based Access Control: A Case Study through Ontology Based Data Access

Ontoloji Tabanlı Erişim Denetimi: Ontoloji Tabanlı Veri Erişimi yoluyla Bir Durum Çalışması

Özgü Can *, Murat Osman Ünalır

Ege Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, İzmir, TÜRKİYE
*Sorumlu Yazar / Corresponding Author **: ozgu.can@ege.edu.tr

Geliş Tarihi / Received: 01.08.2022 *Araştırma Makalesi/Research Article*
Kabul Tarihi / Accepted: 10.10.2022 *DOI:10.21205/deufmd.2023257413*
Atıf şekli/ How to cite: CAN, Ö., ÜNALIR, M.O.(2023). Ontology Based Access Control: A Case Study through Ontology Based Data Access. DEUFMD, 25(74),417-432.

Öz

Ontoloji Tabanlı Veri Erişimi (OBDA), bir ontoloji ile bir veri kaynağı arasında kurulan eşleme sonucunda veri erişiminin ve veri entegrasyonunun sağlanmasıdır. Böylece, Anlamsal Web teknolojileri kullanılarak büyük miktarda verinin depolanması kolaylaşmakta, daha güçlü sorgular yazılabilmekte ve karmaşık bilgi sistemlerinin yönetimi hızlı ve etkin bir şekilde yapılabilmektedir. Ontoloji Tabanlı Erişim Denetimi (OBAC), Anlamsal Web teknolojilerini kullanarak erişim denetim düzeneklerinin uygulanmasını sağlamaktadır. Bu nedenle, veri mahremiyetini korumak için yalnızca yetkilendirilmiş kişiler verilere erişebilmektedir. Bu çalışmada, veri modelinden bağımsız bir erişim denetim yaklaşımı ile veri sanallaştırmayı sağlarken güvenliği artırmak için OBDA ve OBAC entegre edilmiştir. Bu amaçla, sağlık alanı için bir durum çalışması sunulmuştur. Böylelikle, hastane alanı için ilişkisel bir veri tabanı, ilgili hastane veri tabanı için bir Hastane Ontolojisi ve bir erişim denetim politikası oluşturulmaktadır. Ayrıca, hastane veri tabanı ile Hastane Ontolojisi arasındaki ilgili eşleştirmeler Ontop çerçevesi kullanılarak oluşturulmakta ve son olarak, eşleştirmeleri ve erişim kurallarını değerlendirmek için Ontop SPARQL kullanılarak çeşitli sorgular yürütülmektedir.

Anahtar Kelimeler: *Erişim Denetim, Veri Erişimi, Mahremiyet, Ontolji, Anlamsal Web, Bilgi Mühendisliği*

Abstract

Ontology Based Data Access (OBDA) is the provision of data access and data integration as a result of the mapping that is established between an ontology and a data source. Thus, storing large amounts of data becomes easier, more powerful queries can be written, and management of complex information systems can be performed quickly and effectively by using Semantic Web technologies. Ontology Based Access Control (OBAC) uses Semantic Web technologies to enable the enforcement of access control mechanism. Therefore, only authorized persons can access data to protect data privacy. In this study, OBDA and OBAC are integrated to improve security while providing data virtualization with a data model-independent access control approach. Therefore, a use case study for the healthcare domain is presented. Hence, a relational database for the hospital domain, a Hospital Ontology for the related hospital database and an access control policy are created. Also, the relevant mappings between the hospital database and the Hospital Ontology are established by using the Ontop framework and finally, various queries are executed by using Ontop SPARQL to evaluate mappings and access rules.

Keywords: *Access Control, Data Access, Privacy, Ontology, Semantic Web, Knowledge Engineering*

1. Introduction

Today, data production is increasing and a large amount of data is collected in many fields. Health data, social network data, sensor data, and data from many other categories are collected into data repositories. Organizing, analyzing, and evaluating this big data is a necessity to obtain meaningful query results and to access useful information that can be used by decision support systems. On the other hand, digital technologies and the digitization process have led databases to increase in complexity and heterogeneity. Besides, most data sources are heterogeneous and data are published in formats that are not suitable to be directly processed by analytic tools [1]. This makes data integration difficult, whereas data integration is essential for effective data utilization [2]. Ontology Based Data Access (OBDA) is considered an essential component of next-generation information systems and is used to access data stored in the existing data sources. OBDA aims to query databases by using ontologies. Ontology identifies the relevant concepts in a domain that is modeled, creates a common vocabulary for the related domain information, and provides an explicit specification to these concepts. Therefore, an ontology establishes a high-level global data source schema in the OBDA paradigm and enables a vocabulary for user queries [3]. Thus, data access and data integration are provided with a data source, an ontology, and the mapping between the ontology and the data source. Thereby, the technical-schema-level details of the data are abstracted and ontology allows to conceptually specify the data. Also, the mapping of legacy relational data to ontology concepts enables the retrieval of more enriched query results and provides effective data analytics. In this regard, using OBDA and Semantic Web technologies enable effective and reliable sharing of information among various systems to support the decision-making systems.

The governing, curating and sharing of data support decision-making systems, but they are also challenged by security and privacy requirements. Besides, the recent developments in information and communication technologies enable users to access data anytime and anywhere. This connectedness emerges as an important problem in terms of data privacy and data security. Hence, data must be protected from unauthorized access and the ability to provide access control is crucial. For this purpose, access to data should be controlled and limited by authorizing data access. Ontology Based Access Control (OBAC) [4-6] uses Semantic Web technologies to control access to data. Thus, users' access to data is controlled in accordance with the rights/permissions and prohibitions that are defined.

In this study, OBAC and OBDA are integrated to develop a data model-independent access control. Thus, access to data sources is abstracted independent of the underlying mapping. As a result of this abstraction, it is not necessary to understand the structure of data sources during the query process, and the query can be executed on data sources by using ontology and mappings. Therefore, OBDA is represented at the access control level and access to data is controlled to preserve data privacy. This study is based on the conceptual model that is proposed in [7]. In this study, the presented conceptual model is established and queries are executed. For this purpose, a use case study for the hospital domain is presented. The contribution of this paper is enhancing the OBAC model with the OBDA paradigm. The aim of this study is to ensure semantic access to information resources by preventing unauthorized access requests. Therefore, security will be ensured and privacy will be preserved while providing data virtualization.

The rest of the paper is organized as follows: the current state of the field is presented in Section 2, the proposed model is introduced in Section 3 and also a case study of the proposed model for the healthcare domain is presented in Section 3. Section 4 specifies the query results executed on the proposed approach. Finally, Section 5 concludes and clarifies the future studies.

2. Related Work

Database theory and database systems are considered as efficient data storage because of their performance benefits, and therefore contents of a database are brought into the Semantic Web [8]. Hence, OBDA systems and the database-to-ontology mapping problem are studied in a great number of researches in the literature. OBDA abstracts data from the storage details and provides end-users with transparent access to data [9]. For this purpose, OBDA presents a solution through mappings that link properties and classes in the ontology to queries that are executed over the database. In [10], a survey of OBDA systems is presented and an

OBDA system is considered as *a superstructure over a set of the existing sources of structured data*.

OBDA is regarded as an effective semantic approach that deal with vast amounts of heterogeneous complex data in several domains. For instance, in [11], OBDA is used to facilitate data operations in energy technology forecasting. Similarly, an end-to-end OBDA system that provides scalable end-user access to industrial Big Data stores is developed in an EU FP7-funded project named Optique [12, 13]. Also, data access challenges in the data-intensive petroleum company Statoil and the developed solution for these challenges with OBDA are presented in [14]. In [2], an OBDA based framework named Semantic Integration at Bosch (SIB) is proposed. The SIB framework integrates Bosch manufacturing data semantically to support product quality analysis. In [15], an OBDA based framework is presented to enable the access to cultural and historical data about commercial trade system and food production during the Roman Empire. An OBDA based approach is proposed in [16] to combine and process static and real-time data from various sources in the maritime security domain. The primary objective is increasing maritime situation awareness, such as detecting and analyzing suspicious vessel movements and abnormal vessel behaviors. In [17] an approch is proposed for the agriculture domain. The proposed approach aims to bind the farming data sources in Nepal with various external datasets.

In today's information technology environment, it is important to improve the security and privacy of resources. Hence, it is a necessity to authorize data access and define restrictions for access rights. As Semantic Web deals with sensitive data, it is a critical issue to provide a secure Semantic Web. In [18], a review on security and privacy challenges related with Semantic Web technologies is presented. A Semantic Web based security framework must be semantically rich, flexible, and simple to automate [19]. Therefore, a policy management approach and a policy language to define security requirements in Semantic Web are proposed in [19]. In [20], an approach to enable the specification and computation of access control policies for Semantic Web services is proposed. A formal specification for semantic access control and the semantic validation algorithms to detect semantically incomplete or incorrect access control policies are presented in [21]. In [22], the Role Based Access Control (RBAC) model is adopted to Semantic Web technologies and extended with credentials.

In this study, an approach is proposed to enhance the OBDA paradigm by preventing unauthorized access to data. The study aims to improve security and preserve privacy while providing data virtualization. For this purpose, the OBAC model [4-6] is used and integrated with OBDA to control data access requests according to the defined policy rules. The proposed approach is based on the conceptual model that is presented in [7]. To the best of our knowledge, this aspect is not considered in the literature. In the proposed approach, OBAC represents the semantical meaning of the security information and it has the advantage of being a fully semantic access control model. Integrating the OBAC model with OBDA offers a solution to the security and privacy challenges that arise from the OBDA paradigm. The proposed approach is presented with a use case that is based on a hospital domain.

Table 1 presents the existing studies in the literature related with the OBDA approach. Hence, the main contribution of this study is to maintain data security and preserve data privacy while processing data from various heterogeneous sources efficiently. Moreover, the abstraction of data sources in the data later of the systems is maintained with the proposed approach. According to our literature survey, there is no approach that integrates the OBDA paradigm with OBAC for enhancing data security and preserving privacy.

3. Material and Method

This study proposes an architecture that integrates the OBAC model within the scope of OBDA to provide a privacy framework. Figure 1 shows the proposed architecture.

Table 1. The OBDA related studies in the literature.

Tablo 1. OBDA ile ilgili literatürdeki çalışmalar.

Title	**Goal**	**Use Case Domain**
Semantic Integration of Bosch Manufacturing Data Using Virtual Knowledge Graphs [2]	Integrating manufacturing data to perform product quality analysis and enriching answers to user queries	Surface Mounting Process (SMT) – Bosch Manufacturing Data
Ontology-based Data Access for Energy Technology Forecasting [11]	Applying OBDA to Energy Technology Database within technology forecasting information system	Energy Technology
Optique: Towards OBDA Systems for Industry [12] Ontology Based Data Access in Statoil [14]	Developing an end-to-end OBDA system to provide scalable end-user access to industrial Big Data stores	Two use cases and two industrial partners: Siemens and Statoil
Ontology-based data integration in EPNet: Production and distribution of food during the Roman Empire [15]	Enabling the access to cultural and historical data about the commercial trade system and food production during the Roman Empire	Historical data sets (the Epigraphic Database Heidelberg (EDH), the Pleiades dataset, and the EPNet relational repository)
Ontology-Based Data Access for Maritime Security [16]	Combining and processing static and real-time data from various sources, increasing the value of data and improving the processing workflow in the maritime domain	Maritime
Ontology Based Data Access and Integration for Improving the Effectiveness of Farming in Nepal [17]	Obtaining a diversity of related agricultural information to enhance the productivity of agricultural crops in Nepal	Agriculture (Farming datasets)
Ontology Based Access Control: A Case Study through Ontology Based Data Access (*The proposed approach*)	Maintaining data security and preserving privacy	Healthcare

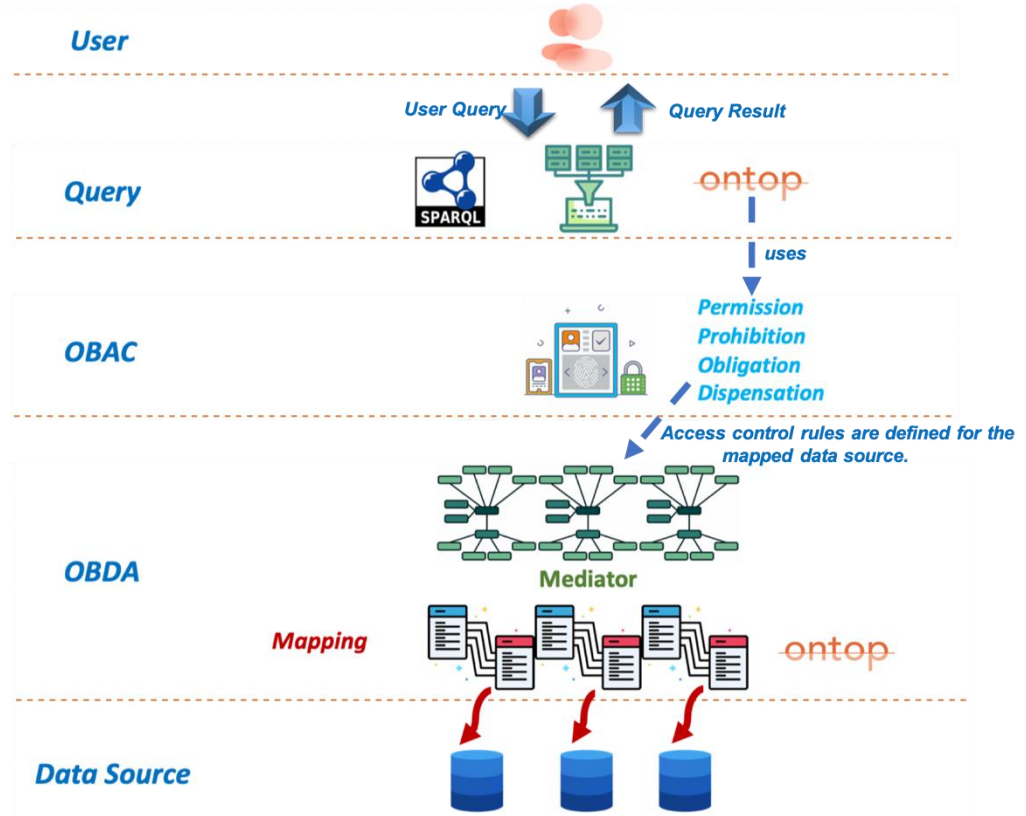

Figure 1. The proposed architecture.

Şekil 1. Önerilen mimari.

The proposed architecture enforces the access control mechanism for the OBDA. Therefore, it enables OBDA to preserve privacy based on the OBAC model.

In the OBDA paradigm, different data sets are integrated with an ontology. In this paradigm, ontology provides the conceptualization for the data access and it is mapped to the data source. Therefore, OBDA is based on three components: data source, ontology, and mappings. The data source is described through schemes and related information, ontology is the representation of the conceptual domain and mapping is the correspondence between the ontology and data sources [23].

In OBDA, users access data sources through a conceptual layer and perform their queries. The related conceptual layer is an OWL or RDF ontology and uses R2RML mappings to connect to the underlying database.

R2RML is a language that expresses customized mappings from relational databases to RDF datasets [24]. When the related ontology is queried with SPARQL [25], the OBDA system retrieves the elements from the data sources and uses the related mappings to generate the query answers.

In OBAC [6], policies are represented with deontic concepts. OBAC allows to create, modify, and delete policy ontologies. For this purpose, OBAC uses Rei policy specification language. Users can specify and represent the concepts of permissions, prohibitions, obligations, and dispensations by using Rei [19, 26, 27]. Developers can express different kinds of domain-independent policy ontologies. In OBAC, policy ontologies include policy objects, subjects, and objects. There are four policy objects in OBAC: Permissions, Prohibitions, Obligations, and Dispensations. A Permission policy object indicates actions that an entity can do; a Prohibition policy object indicates actions that an entity can't do; an Obligation policy object indicates actions that an entity should do; a Dispensation policy object indicates actions that

an entity need no longer do. A policy is shown with a **(S,O,A)** triple. A subject (**S**) indicates the user who requests access to a resource, an object (**O**) specifies the resource which is going to be accessed and an action (**A**) specifies the operations which the subject requests to achieve on a resource.

The proposed model is based on a materialization-based approach (forward chaining) [7]. In the materialization-base approach [28], the database **D** is the input, **O** is the target ontology and the mapping from **D** to **O** is **M**. The legacy data source is the ABox **(A)** and the ontology is the TBox **(T)**. The SPARQL query **Q** is executed over the **D**, **O**, and **M**. Therefore, the access to the underlying data sources is abstracted independent of the mapping. The mapping between a database and an ontology is achieved by Ontop framework [29]. Ontop is an open-source OBDA framework and a query transformation module. Hence, queries are executed by using the Ontop framework.

Ontop is a virtual knowledge graph system that enables any relational database's content available as knowledge graphs. For this purpose, Ontop converts SPARQL queries issued across knowledge graphs into SQL queries executed by relational data sources. Ontop rewrites the SPARQL query into SQL query, delegates execution of the SQL query to the data source and returns the query result [30]. Thus, data stays in the original data source instead of being transferred to another database. The following example defines the mapping for patients in the database:

Target:

```
:hospital/patient/{patientID}
a :Patient;
a :patientID{PatientID};
a :name{name};
a :lastname{lastname} .
```

Source (SQL Query):

```
SELECT patient.name,
       patient.lastname
FROM patient
```

The target of the mapping indicates how to generate the ontology concepts (classes, object and datatype properties). The source of the mapping is the SQL query that retrieves data from the database.

After defining the related mapping, the following SPARQL query will list the patients in the database.

```
SELECT     DISTINCT     ?patientID
?patientname ? patientlastname

WHERE
{
?patient        hospital:patientID
?patientID .
?patient      hospital:patientName
?patientname .
?patient  hospital:patientLastname
?patientlastname .
}
```

3.1. Integrating OBAC with OBDA: A Use Case

In this study, the OBAC model is applied within the scope of OBDA to prevent unauthorized access and to preserve privacy while providing data virtualization. For this purpose, a use case for a hospital domain is performed. In the scope of the use case, the steps adhered are as follows: a hospital database is created, a hospital ontology is developed, a hospital policy ontology is created for the related hospital ontology, the relevant mappings between the policy ontology and the created database are established by utilizing the Ontop framework [28], and various queries are written using Ontop SPARQL. Ontop is an open-source platform to query databases through ontologies. Ontop relies on R2RML mappings, translates SPARQL queries into SQL queries that are executed by the relational data sources, and executes SPARQL queries. In this study, ontologies are created with Protégé ontology editor [31].

First, the hospital database is created by using the MySQL database management system [32]. The Enhanced Entity-Relationship (EER) diagram is given in Figure 2. The created tables are as follows: `action`, `appointments`, `basicscience`, `bloodtests`, `departments`, `doctor`, `doctorpatient`, `equipments`, `granting`, `invoice`, `laboratory`, `laboratorytechnician`, `mechanicaltechnician`, `medicalscience`, `medicalstudent`, `nurse`, `officer`, `patient`, `permission`, `prescriptions`, `prohibition`, `radiologytechnician`, `room`, `surgicalscience`. Also, sample data are inserted into tables.

Later, Hospital Ontology and Hospital Policy Ontology are created. While creating Hospital Ontology the relevant classes are created according to the tables in the Hospital Database. The classes and subclasses in Hospital Ontology are as follows: `Acounting`, `Administration`, `Appointments`, `Departments`, `BasicScience`, `MedicalScience`, `SurgicalScience`, `Documents`, `HealthReports`, `Prescriptions`, `Results`, `BloodTests`, `RadiologyResults`, `CAT`, `CT`, `Mammography`, `MRA`, `MRI`, `PET`, `XRay`, `UrineTests`, `VaccinationCard`, `Equipments`, `Laboratory`, `Patient`, `Room`, `Staff`, `Doctor`, `Intern`, `MedicalStudent`, `Nurse`, `Officer`, `Technician`, `LaboratoryTechnician`, `MechanicalTechnician`, `RadiologyTechnician`, `UltrasoundTechnician`.

The classes, object and data type properties of Hospital Ontology are shown in Figure 3, 4 and 5, respectively. The overview of the Hospital Ontology is given in Figure 6.

The Hospital Policy Ontology is created based on the Hospital Ontology which is the domain ontology of the use case study. The classes of the Hospital Policy Ontology is given in Figure 7.

The actions that can be perfomed on hospital data are presented in `Action` class. The defined actions of the related class are as follows: `CreatingInvoice`, `DeletingInvoice`, `EditingDocuments`, `EditingInvoice`, `EditingResults`, `EditVaccinationCalendar`, `ViewPrescription`, `ViewResults`, `ViewVaccinationCalendar` and `WritingPrescription`.

In the Hospital Policy Ontology, `Policy`, `Permission`, `Prohibition`, `Granting`, and `SimpleConstraint` classes are created to specify the access rights and actions that can be performed on the hospital data.

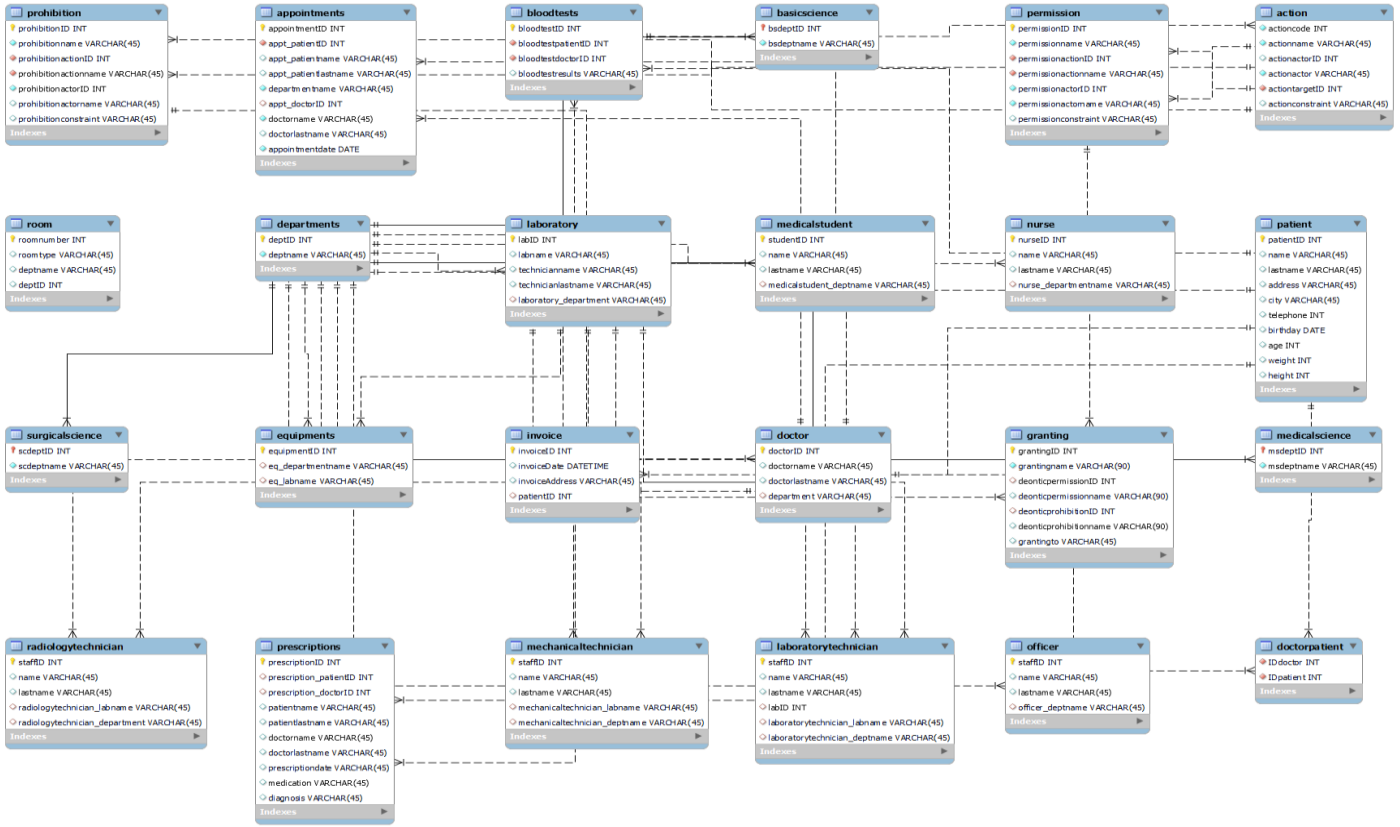

Figure 2. The hospital database.

Şekil 2. Hastane veritabanı.

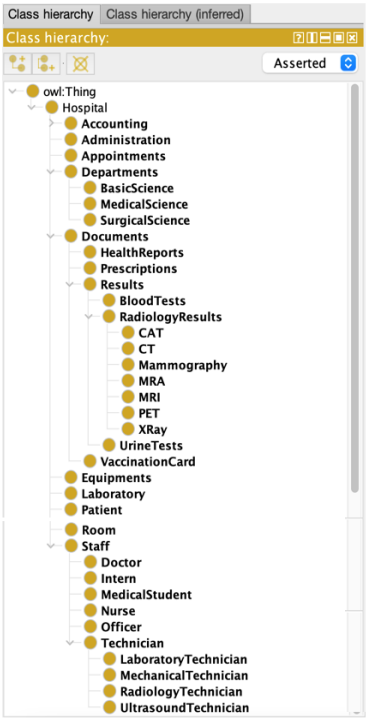

Figure 3. The class hierarchy of Hospital Ontology.

Şekil 3. Hastane Ontolojisi'nin sınıf hiyerarşisi.

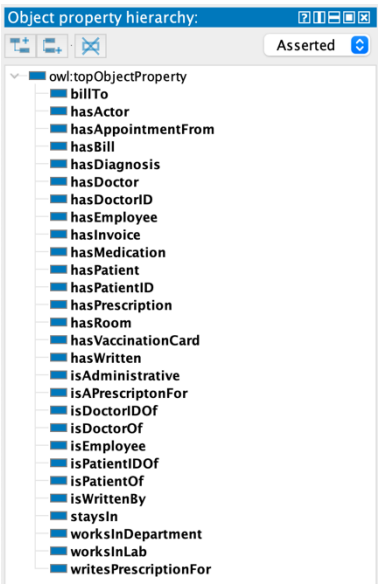

Figure 4. The object properties of Hospital Ontology.

Şekil 4. Hastane Ontolojisi'nin nesne özellikleri.

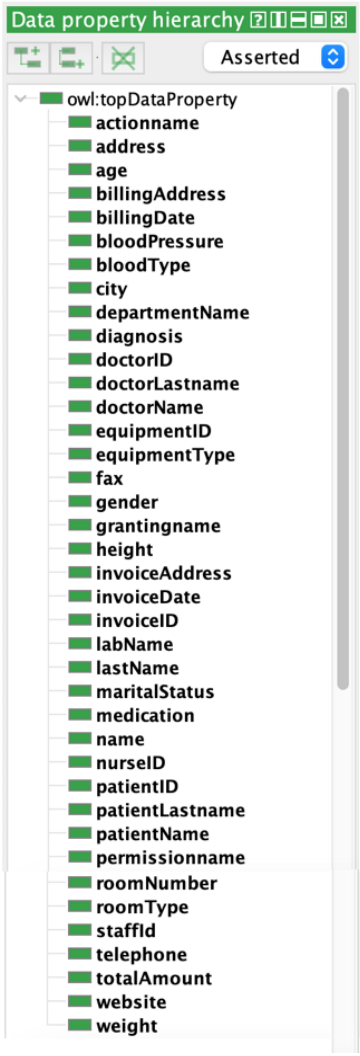

Figure 5. The data properties of Hospital Ontology.

Şekil 5. Hastane Ontolojisi'nin veri özellikleri.

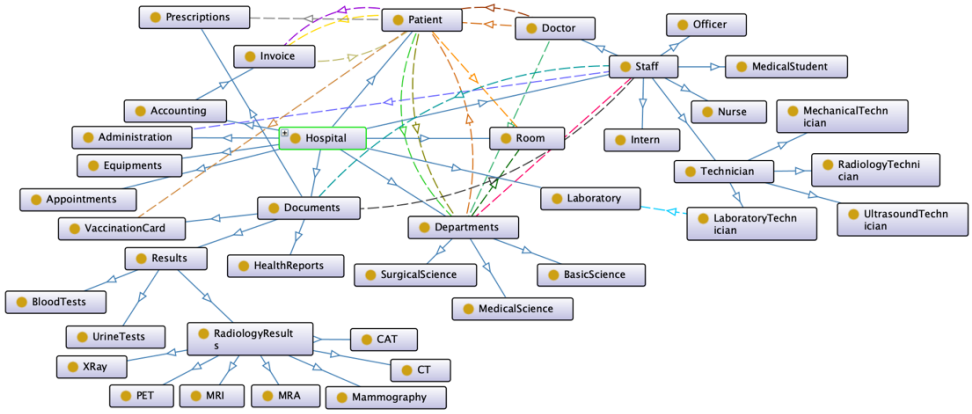

Figure 6. The overview of the Hospital Ontology.

Şekil 6. Hastane Ontolojisi'nin genel görünümü.

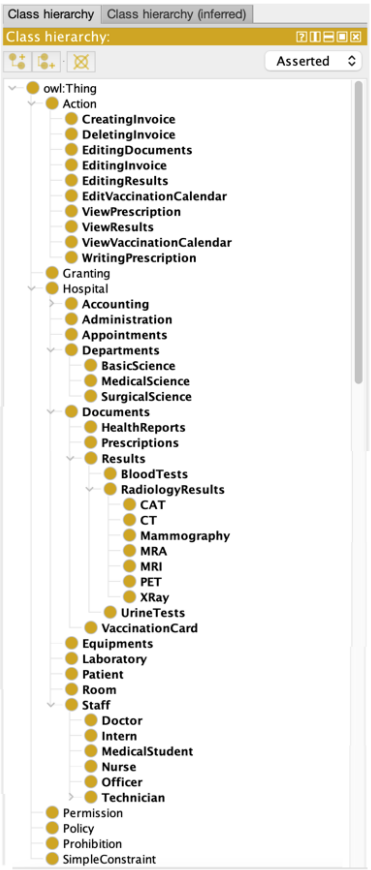

Figure 7. The class hierarchy of Hospital Policy Ontology.

Şekil 7. Hastane Politika Ontolojisi'nin sınıf hiyerarşisi.

After creating the Hospital Policy Ontology, mappings between the Hospital Database and the Hospital Policy Ontology are established. An example mapping of doctor-patient relationship is shown in Figure 8. In Figure 9, a mapping for doctors' access permissions is shown. Figure 10 shows the mapping for prohibitions. The list of defined mapping is given in Figure 11. After the mapping, the integration of OBAC with OBDA is finalized.

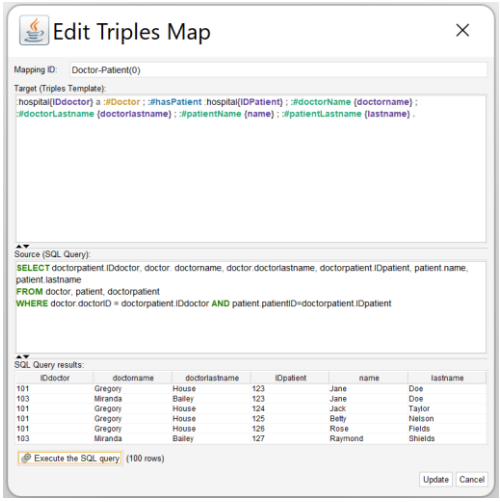

Figure 8. The mapping for Doctor-Patient relationship.

Şekil 8. Doktor-Hasta ilişkisi için eşleme.

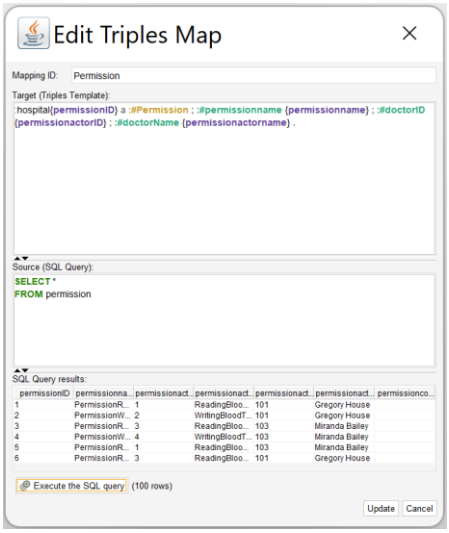

Figure 9. The mapping for Permissions.

Şekil 9. İzinler için eşleme.

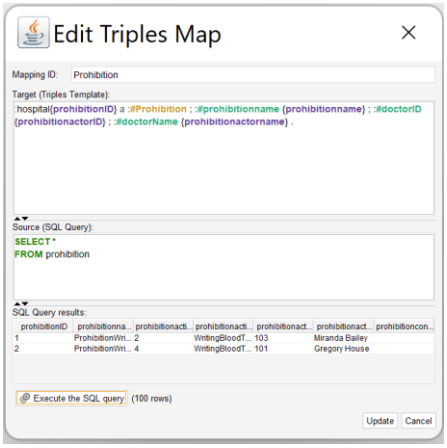

Figure 10. The mapping example for Prohibitions.

Şekil 10. Yasaklar için eşleme.

4. Results

The related studies presented in this article are obtained on a machine with specifications of Intel(R) Core(TM) i7-8550U CPU @ 1.80GHz 1.99 GHz, 16GB RAM.

The Hospital Policy Ontology metrics are presented n in Figure 11. The defined mappings between the Hospital Database and Hospital Policy Ontology are displayed in Figure 12. In order to validate the integration process of OBAC with OBDA and the defined mappings, SPARQL queries are executed. For this purpose, Ontop SPARQL Manager is used.

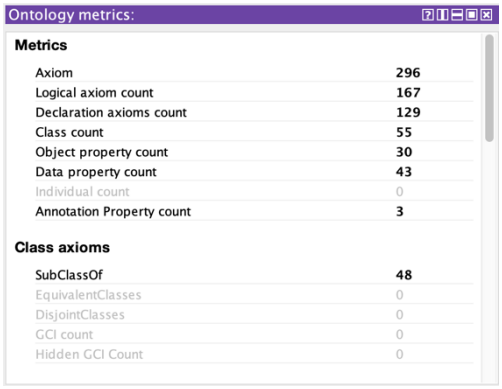

Figure 11. The ontology metrics for the Hospital Policy Ontology.

Şekil 11. Hastane Politika Ontolojisi için ontoloji metrikleri.

Thence, queries of the defined mappings are written and executed. Figure 13, Figure 14 and Figure 15 represent the SPARQL queries of the mappings that are displayed in Figure 8, Figure 9 and Figure 10, respectively.

In Figure 13, the doctor-patient relationship is queried. The query results list patients' doctors. Thus, doctor's ID, doctor name and surname, patient's ID, patient name and surname are shown.

Figure 14 and Figure 15 present the query results for the specified policy definitions that are defined for doctors. The query results presented in Figure 13 show the access permissions for doctors in the Hospital Database. Thus, permissions, the ID and name of actors who are permitted to perform the related action are listed as the query result.

Similarly, Figure 15 present the defined prohibitions for doctors. The query results list the defined prohibitions, the ID and name of the actors who are prohibited for the related action.

Consequently, these query results show that data access is controlled by performing OBAC on the OBDA approach. Thus, a privacy-aware OBDA approach is applied by integrating OBAC with OBDA.

Figure 12. The defined mappings.

Şekil 12. Tanımlanan eşlemeler.

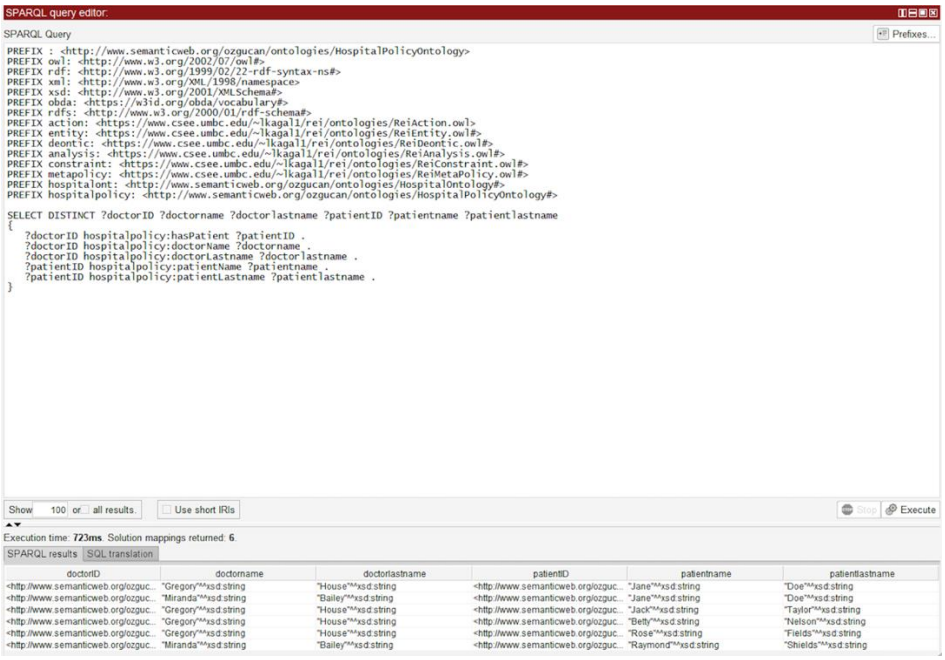

Figure 13. The SPARQL query results for listing patients' doctors.

Şekil 13. Hastaların doktorları listelemek için SPARQL sorgu sonuçları.

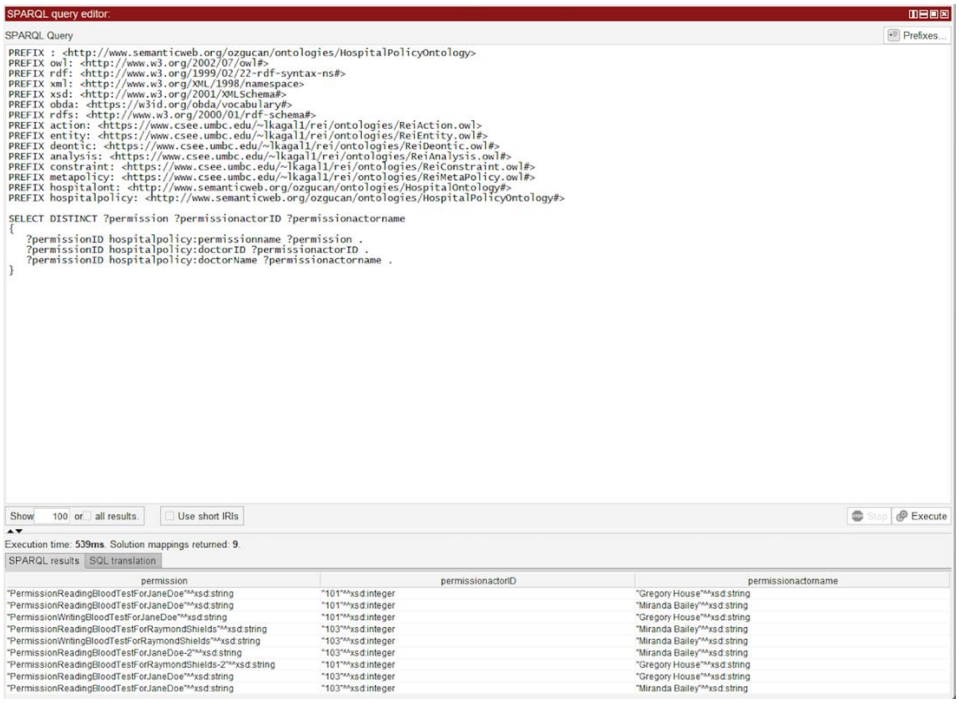

Figure 14. The SPARQL query results for doctors' permissions.

Şekil 14. Doktorların izinleri için SPARQL sorgu sonuçları.

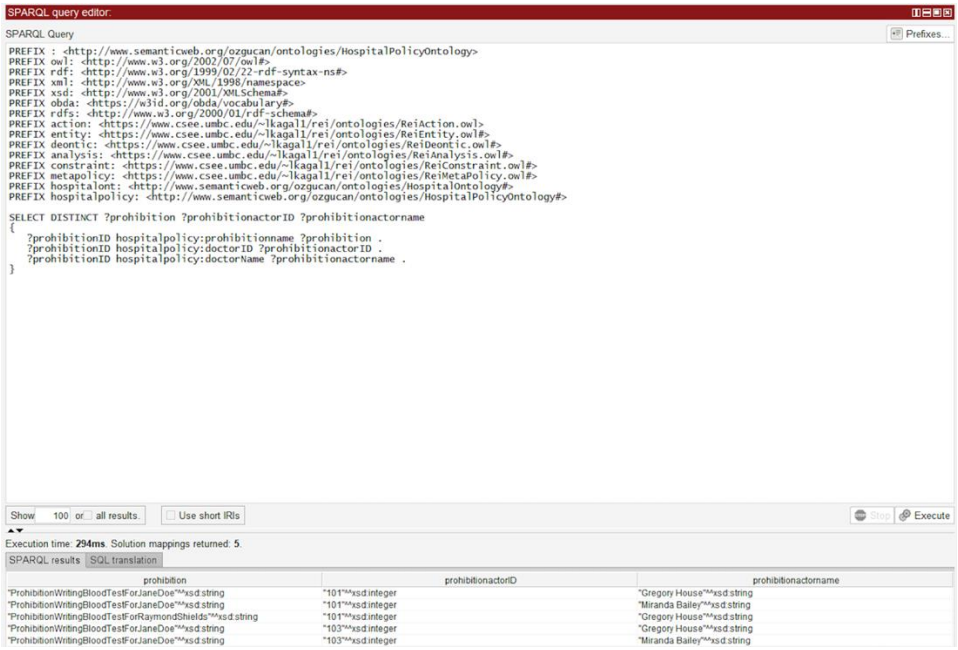

Figure 15. The SPARQL query results for doctors' prohibitions.

Şekil 15. Doktorların yasakları için SPARQL sorgu sonuçları.

5. Conclusion and Future Work

OBDA is an ontology-based interface to connect a data source and an ontology. Hence, OBDA provides data access and data integration as a result of a data source, an ontology, and the mapping between the data source and the ontology. In the OBDA paradigm, ontology is used as a conceptual schema of the interested domain. As OBDA is a mediator between database contents and ontologies, it should be ensured that only authorized persons can access data. In this study, this ensurance is provided by integrating the OBAC model with the OBDA approach. OBAC is a Semantic Web based policy management model to control access to data. The primary purpose of this study is to develop a privacy-aware OBDA solution while abstracting access to data sources independent of the underlying mapping. Therefore, a use case study is presented for the hospital domain.

As future work, Role Based Access Control (RBAC) model will be integrated into the proposed approach by mapping RBAC concepts to the OBAC model. Also, new policy definitions will be created, the related mappings will be established and queries will be executed. Moreover, the OBAC model will be extended with the organizational privacy concepts to enhance the privacy of the OBDA based systems.

5. Sonuç ve Gelecek Çalışmalar

OBDA, bir veri kaynağı ile bir ontolojiyi birbirine bağlayan ontoloji tabanlı bir arayüzdür. Bu nedenle OBDA, bir veri kaynağı, bir ontoloji ve veri kaynağı ile ontoloji arasındaki eşlemenin bir sonucu olarak veri erişimini ve veri entegrasyonunu sağlamaktadır. OBDA paradigmasında ontoloji, ilgilenilen alanın kavramsal bir şeması olarak kullanılmaktadır. OBDA, veritabanı içerikleri ile ontolojiler arasında bir aracı olduğundan, verilere yalnızca yetkili kişilerin erişebilmesi sağlanmalıdır. Bu çalışmada OBAC modeli ile OBDA yaklaşımı entegre edilerek bu güvence sağlanmıştır. OBAC, verilere erişimi kontrol eden Anlamsal Web tabanlı bir politika yönetim modelidir. Bu çalışmanın temel amacı, veri kaynaklarına erişimi alttaki eşlemeden bağımsız olarak soyutlarken mahremiyet-farkında bir OBDA çözümü geliştirmektir. Bu nedenle, hastane etki alanı için bir kullanım durumu çalışması sunulmuştur.

Gelecek çalışma olarak, Rol Tabanlı Erişim Denetim (RBAC) kavramları OBAC modeline eşlenerek RBAC modeli önerilen yaklaşıma entegre edilecektir. Ayrıca, yeni politika

tanımları oluşturulacak, ilgili eşlemeler yapılacak ve sorgular yürütülecektir. Ek olarak, OBDA tabanlı sistemlerin mahremiyetini artırmak için OBAC modeli kurumsal mahremiyet kavramlarıyla genişletilecektir.

6. Ethics Committee Approval and Conflict Of Interest Statement

There is no need to obtain an ethics committee approval for the presented article.

There is no conflict of interest with any person/institution in the presented article.

Acknowledgment

This study is supported by Ege University Scientific Research Projects Committee under the grant number 18-MUH-036.

References

[1] Haw, S.C, May, J.W., Subramaniam, S. 2017. Mapping Relational Databases to Ontology Representation: A Review. In: Proceedings of the International Conference on Digital Technology in Education (ICDTE'17), pp.54-55. DOI: 10.1145/ 3134847.3134852

[2] Kalayci E.G. et al. 2020. Semantic Integration of Bosch Manufacturing Data Using Virtual Knowledge Graphs. In: Pan J.Z. et al. (eds) The Semantic Web-International Semantic Web Conference (ISWC 2020). Lecture Notes in Computer Science, Vol 12507, pp. 464-481. Springer, Cham. DOI: 10.1007/978-3-030-62466-8_29

[3] Kontchakov, R., Rodrguez-Muro, M., Zakharyaschev, M. 2013. Ontology-Based Data Access with Databases: A Short Course. In: Rudolph, S., Gottlob, G., Horrocks, I., van Harmelen, F. (eds) Reasoning Web-Semantic Technologies for Intelligent Data Access (Reasoning Web 2013). Lecture Notes in Computer Science, Vol 8067, pp. 194-229. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-39784-4_5

[4] Can, O. 2009. Personalizable Ontology Based Access Control for Semantic Web and Policy Management (Anlamsal Web için Kişiselleştirilebilir Ontoloji Tabanlı Erişim Denetimi ve Politika Yönetimi). PhD Thesis, Ege University, Department of Computer Engineering.

[5] Can, O., and Unalir, M.O. 2010. Ontology Based Access Control. Pamukkale University Journal of Engineering Sciences, 162:197-206.

[6] Can, O., Bursa, O., and Unalir, M.O. 2010. Personalizable Ontology Based Access Control. Gazi University Journal of Science, 23(4):465-474.

[7] Can, O., and Unalir, M.O. 2022. Revisiting Ontology Based Access Control: The Case for Ontology Based Data Access. In: Proceedings of the 8th International Conference on Information Systems Security and Privacy (ICISSP 2022), 515-518. DOI: 10.5220/0010898100003120

[8] Spanos, D.E., Stavrou, P., and Mitrou, N. 2012. Bringing relational databases into the Semantic Web: A survey Semantic Web, 3(2):169-209.

[9] Lanti, D., Xiao, G., Calvanese, D. 2016. Fast and Simple Data Scaling for OBDA Benchmarks. In: Proceedings of the Workshop on Benchmarking Linked Data (BLINK 2016), Volume 1700 of CEUR Workshop Proceedings.

[10] Kogalovsky, M.R. 2012. Ontology-based data access systems. Programming and Computer Software, 38:167–182.

[11] Mikheev, A.V. 2018. Ontology-based Data Access for Energy Technology Forecasting. In: Proceedings of the Vth International workshop on Critical infrastructures: Contingency management, Intelligent, Agent-based, Cloud computing and Cyber security (IWCI 2018), Vol. 158. DOI: 10.2991/iwci-18.2018.26

[12] Kharlamov E. et al. 2013. Optique: Towards OBDA Systems for Industry. In: Cimiano, P., Fernández, M., Lopez, V., Schlobach, S., Völker, J. (eds) The Semantic Web: ESWC 2013 Satellite Events, LNCS, Vol 7955, 125-140, Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-41242-4_11

[13] Giese, M. et al. 2013. Scalable End-user Access to Big Data. Rajendra Akerkar (Edt) Big Data Computing. 1st Edition. Chapman and Hall/CRC , New York.

[14] Kharlamov, E. et al. 2017. Ontology Based Data Access in Statoil. Journal of Web Semantics, 44, pp. 3-36.

[15] Calvanese, D. et al. 2016. Ontology-based data integration in EPNet: Production and distribution of food during the Roman Empire. Engineering Applications of Artificial Intelligence, 51:212-229.

[16] Brüggemann, S., Bereta, K., Xiao, G., and Koubarakis, M. 2016. Ontology-Based Data Access for Maritime Security. In: Sack, H., Blomqvist, E., d'Aquin, M., Ghidini, C., Ponzetto, S., Lange, C. (eds) European Semantic Web Conference (ESWC2016): The Semantic Web-Latest Advances and New Domains. Lecture Notes in Computer Science, Vol 9678, pp. 741-757. Springer, Cham. DOI: 10.1007/978-3-319-34129-3_45

[17] Pokharel, S., Sherif, M. A., and Lehmann, J. 2014. Ontology Based Data Access and Integration for Improving the Effectiveness of Farming in Nepal, In: 2014 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT), pp. 319-326.

[18] Kirrane, S., Villata, S., and d'Aquin, M. 2018. Privacy, security and policies: A review of problems and solutions with semantic web technologies. Semantic Web, 9(2):153-161.

[19] Kagal, L., Finin, T., and Joshi, A. 2003. A Policy Based Approach to Security for the Semantic Web. In: Fensel D., et al. (eds) The Semantic Web - International Semantic Web Conference (ISWC 2003), LNCS, Vol 2870, pp. 402-418. DOI: 10.1007/978-3-540-39718-2_26

[20] Agarwal, S., and Sprick, B. 2004. Access control for semantic Web services. In: Proceedings of IEEE International Conference on Web Services, pp. 770-773.

[21] Yagüe, M.I., Gallardo, M.M., and Mana, A. 2005. Semantic Access Control Model: A Formal Specification. In: In: di Vimercati, S.d.C., Syverson, P., Gollmann, D. (eds) Computer Security – ESORICS 2005. Lecture Notes in Computer Science, Vol 3679,

pp. 24-43. Springer, Berlin, Heidelberg. DOI: 10.1007/ 11555827_3

[22] He Z., Huang, K., Wu, L., Li, H., and Lai, H.. 2010. Using Semantic Web Techniques to Implement Access Control for Web Service. In: Zhu R., et al. (eds) International Conference on Information Computing and Applications (ICICA 2010), CCIS, Vol 105, pp 258-266. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-16336-4_34

[23] Daraio, C., Lenzerini, M., Leporelli, C. et al. 2016. The advantages of an Ontology-Based Data Management approach: openness, interoperability and data quality. Scientometrics, 108:441-455.

[24] W3C Recommendation: R2RM. 2012. https://www.w3.org/TR/r2rml (Access Date: 25.07.2022)

[25] W3C Recommendation: SPARQL Query Language for RDF. 2008. https://www.w3.org/TR/rdf-sparql-query (Access Date: 25.07.2022)

[26] G. Tonti, J.M. Bradshaw, R. Jeffers, R. Montanari, N. Suri, A. Uszok, A., ``Semantic Web Languages for Policy Representation and Reasoning: A Comparison of KAoS, Rei, and Ponder,'' in ISWC 2003, Vol 2870, pp. 419--437, Springer, 2003.

[27] Kagal, L. 2002. Rei: A Policy Language for the Me-Centric Project. TechReport.

[28] Sequeda, J.F. 2017. Integrating Relational Databases with the Semantic Web: A Reflection. In: Ianni G. et al. (eds) Reasoning Web 2017: Semantic Interoperability on the Web. LNCS, Vol 10370, pp. 68-120, Springer, Cham. DOI: 10.1007/978-3-319-61033-7_4

[29] Ontop Framework. 2022. https://ontop-vkg.org. (Access Date: 25.07.2022)

[30] Calvanese, D., Cogrel, B. Komla-Ebri, S., Kontchakov, R., Lanti, D., Rezk, M., Rodriguez-Muro, M., Xiao, G. 2017. Ontop: Answering SPARQL Queries over Relational Databases. Semantic Web Journal, 8(3):471–487.

[31] Protégé Ontology Editor. 2022. https://protege.stanford.edu (Access Date: 25.07.2022)

[32] MySQL. 2022. https://www.mysql.com (Access Date: 25.07.2022)