

# An Ontology based Personalized Privacy Preservation

Ozgu Can<sup>a</sup> and Buket Usenmez

Department of Computer Engineering, Ege University, 35100 Bornova-Izmir, Turkey

**Keywords:** Data Anonymization, Data Privacy, Data Security, Knowledge Engineering, Ontology, Semantic Web.

**Abstract:** Various organizations share sensitive personal data for data analysis. Therefore, sensitive information must be protected. For this purpose, privacy preservation has become a major issue along with the data disclosure in data publishing. Hence, an individual's sensitive data must be indistinguishable after the data publishing. Data anonymization techniques perform various operations on data before it's shared publicly. Also, data must be available for accurate data analysis when data is released. Therefore, differential privacy method which adds noise to query results is used. The purpose of data anonymization is to ensure that data cannot be misused even if data are stolen and to enhance the privacy of individuals. In this paper, an ontology-based approach is proposed to support privacy-preservation methods by integrating data anonymization techniques in order to develop a generic anonymization model. The proposed personalized privacy approach also considers individuals' different privacy concerns and includes privacy preserving algorithms' concepts.

## 1 INTRODUCTION


Organizations share information publicly for statistical and academic research objectives. This sensitive statistical data has a substantial importance. Hence, adversaries can discover individuals' identities by analysing the released data and thereby privacy breaches can occur. On the other hand, data analysis process offers significant benefits. Therefore, there should be a balance between providing the usefulness of the released data and protecting the privacy of the owner of these data. In order to achieve this balance, data must be published in a privacy-preserving way.

A guideline is published by the National Institute of Standards and Technology (NIST) in order to protect personally identifiable information (PII). PII is any information about the individual that can be used to distinguish the individual's name, social security number, date and place of birth or any other information that is linked or linkable to an individual, such as medical, educational and financial information (McCallister et al., 2010). Furthermore, the significant benefits of data analysis cannot be ignored. However, individuals' privacy must be protected by maintaining data analysis with minimal loss of personal information. Thus, various privacy-preserved data publishing methods have been

proposed. Differential privacy (Dwork, 2008), k-anonymity (Ciriani et al., 2007), l-diversity (Machanavajjhala et al, 2007) and t-closeness (Li et al., 2007) are techniques to provide privacy-preserving data publishing. These privacy-preserving data publishing methods ensures privacy protection against data disclosure by publishing useful information while preserving data privacy.

In this work, an ontology-based privacy-preservation model is proposed in order to combine the main concepts of the existing anonymization methods. For this purpose, the main concepts of the existing anonymization methods are analysed to conceptualize a generic anonymization model. Thus, the proposed ontology-based privacy-preservation model will serve as a base privacy model and new anonymization methods will be easily integrated to the proposed privacy model.

Another important issue while protecting privacy and releasing information is enhancing individuals' privacy concerns. Individuals may have different privacy concerns about their sensitive data. For example, an individual may classify her age information with low level and her location information with high level privacy degrees. The proposed privacy preservation model has a personalized view that allows different levels of data privacy. The privacy-preserving data publishing

<sup>a</sup> <https://orcid.org/0000-0002-8064-2905>

method that will be applied on an individual data set will be enforced according to the individual's personal privacy preferences. The goal of the proposed privacy-preservation model is to maintain a relation between personalization and data anonymization methods. Therefore, individuals' personal privacy expectations will be met by using different privacy levels. Also, the proposed model guarantees privacy-preserved query results and ensures personalized privacy. In this work, we created an ontology and executed queries for the model presented in (Usenmez and Can, 2015). Additionally, a case study is presented. The rest of this paper is organized as follows. In Section 2, the current researches are introduced. In Section 3, the proposed ontology-based privacy-preservation model is described and exemplified. Because of its nature, healthcare domain has quite personal information, and patients usually prefer to protect their privacy from others as a basic human desire to live free of intrusion, judgment and prejudice (Project Health Design, 2009). Hence, we used healthcare domain for the exemplification of our work. In Section 4, a case study is presented. In Section 5, example queries are processed on the proposed ontology. Finally, the paper is concluded and the future work is presented in Section 6.

## 2 RELATED WORK

Numerous techniques have been proposed to provide individual privacy while sharing or querying data sets. Differential privacy approach protects original data and changes the result of query by adding a noise. In differential privacy, the researcher studies on real data and generates statistical results. When a query is executed on a data set, differential privacy method adds noise to the query result. For this purpose, the sensitivity of the query is measured. Sensitivity is a metric that expresses how much noise will be added to the query result in order to enhance the distance between similar inputs and to protect individual's privacy on a statistical database. Differential privacy guarantees to learn nothing about an individual while learning useful information about a population (Dwork and Roth, 2014). Differential privacy ensures to protect privacy while releasing data and to provide the optimum transformation on data or statistical result. Therefore, privacy-preserving data analysis is provided. (Sarathy and Muralidhar, 2011) provides an evaluation for the privacy and utility performance of Laplace noise addition to numeric data.

Privacy preserving data mining methods enables knowledge to be extracted from data while protecting the privacy of individuals. There are several researches in the literature related with privacy preserving data mining. In (Mendes and Vilela, 2017), a comprehensive the most relevant privacy preserving data mining techniques in the literature are presented and the current challenges in the related field are discussed. The most known methods are k-anonymity, l-diversity and t-closeness privacy models.

In the k-anonymity model, if each information contained in the released dataset cannot be distinguished from at least  $k-1$  tuples that appears in the released data set, then the dataset is  $k$ -anonymous (Sweeney, 2002). (Ciriani et al., 2007) describes generalization and suppression approaches in order to provide k-anonymity. An enhanced k-anonymity model is proposed in (Wong et al., 2006) to protect identifications and sensitive relationships in a dataset. (Kenig and Tassa) proposes an alternative k-anonymity algorithm to achieve lower information losses.

The l-diversity privacy model that expands the k-anonymity model is proposed in order to provide stronger notion of privacy. (Machanavajjhala et al, 2007) showed two attacks, the homogeneity attack and the background knowledge attack, in order to compromise a k-anonymous dataset. The l-diversity model requires that each equivalence class to have at least  $l$  different values for the sensitive attributes. (Kern, 2013) proposes a model based on l-diversity to reason about privacy in microdata and applies the proposed l-diversity model to a real database.

(Li et al., 2007) showed that the l-diversity has a number of limitations and proposed the t-closeness privacy model that requires the distribution of a sensitive attribute in any equivalence class is close to the distribution of the attribute in the overall table, where close means a threshold  $t$ . In (Ruggieri, 2014), t-closeness is used for discrimination-aware data mining. As stated in (Kern, 2013), each privacy model has its own advantages and disadvantages that have to be considered when applying such principles to microdata. Therefore, (Soria-Comas and Domingo-Ferrer, 2013) connects the k-anonymity, differential privacy and t-closeness privacy models, and also proposes a method to improve the utility of data and to raise the risk of attribute disclosure.

In order to provide a semantic understanding, Semantic Web based studies for privacy preserving data mining also exist in the literature. (Martinez et al., 2010) proposes a masking method for unbounded categorical attributes. (Ayala-Rivera et al., 2017)

presents an evaluation for the quality of generalization hierarchies for categorical data in order to improve their effectiveness for anonymizing data. For this purpose, ontologies are used as an external source of knowledge for the evaluation. In (Miracle and Cheatham, 2016), Semantic Web technologies are used to facilitate record linkage attacks against anonymized datasets. Also, a domain dependent Semantic Web based k-anonymity model is presented in (Omran et al, 2009).

In addition to preserving privacy, providing a personalized privacy is an important issue. As individuals have different privacy concerns, personalized privacy is also needed in data anonymization. (Can, 2018) proposes a personalized anonymity model to provide different privacy levels. In (Gedik and Liu, 2008), a location privacy framework based on personalized k-anonymity model is proposed. A framework for personalized anonymity is also proposed in (Xiao and Tao, 2006).

In our work, we gather differential privacy, k-anonymity, l-diversity and t-closeness privacy preservation models together and perform a personalized privacy preservation by using Semantic Web technologies to enable machine-processable semantics of data. The proposed model is domain independent and provides a personalized privacy in order to meet individuals' different privacy needs. When the proposed model is compared with the existing works, it is seen that the proposed privacy preserving model presents a holistic approach that is composed of: (i) independent of domain (ii) combination of k-anonymity, l-diversity and t-closeness privacy preservation techniques (iii) personalized privacy and (iv) based on Semantic Web technologies.

### 3 AN ONTOLOGY FOR PERSONALIZED PRIVACY PROTECTION

Privacy preservation algorithms have different concepts to provide data protection. The personalized privacy preservation ontology represents the main concepts of anonymization methods semantically and conceptualizes a generic personalized anonymization method. The proposed ontology has the following entities (Usenmez and Can, 2015): Anonymized DataSet, Attribute, DataOwner, DataSet, Domain, DomainLevel, PrivacyConstant, PrivacyLevel, PrivacyMethod, Query, QueryResult and Value. Anonymized

DataSet is the anonymized DataSet. For this purpose, an anonymization algorithm is applied to DataSet. DataSet represents a collection of data and researchers can perform queries on the DataSet. DataOwner is the owner of the data that is represented in the DataSet. Attribute is the information about the data. The Attribute of data change according to the DataSet that is going to be anonymized. For example, while one DataSet may have age, zipcode and diagnose attributes, the other may have birth date, location and treatment attributes. Attribute concept has three subconcepts: Identifier, QuasiIdentifier and SensitiveAttribute. Identifier identifies data uniquely and allows to be able to access to personal data. For example, social security number which is unique to a person is an Identifier and is used to access an individual's personal data. QuasiIdentifier is not an identifier by itself. However, when QuasiIdentifier is used with other attributes it can expose the sensitive information. SensitiveAttribute is used to represents DataOwner's sensitive data that would lead to a privacy leakage when the data set is released. PrivacyMethod represents the data anonymization method and it has subconcepts of k-anonymity, l-diversity, t-closeness and differentialPrivacy. PrivacyConstant is the value of the applied data anonymization method. If k-anonymity is used as the data anonymization method, then a data type property named as kValue; if l-diversity is used, then a data type property named as lValue; if t-closeness is used, then a data type property named as tValue are used. If the used data anonymization method is differential Privacy, then a data type property named as Noise is used. Noise is the value that is going to be added to the query results. PrivacyLevel is used for all types of Attribute and it has subconcepts of VeryHigh, High, Medium, Low and VeryLow. VeryHigh means that the value must be hidden and VeryLow means that the value does not need to be protected. Also, the anonymization methods need a hierarchical generalization tree for DataSet attributes of the related domain. Therefore, Domain concept is used to generalize the hierarchical tree. The DomainLevel is used to represent the level of the hierarchical tree for the Domain concept. Value is the DataOwner's value for an Attribute and it has one subconcept which is AnonymizedValue. After applying the anonymization method,

AnonymizedValue is used to represent the new anonymized value. The queries that are posed on DataSet or AnonymizedDataSet are represented with the Query. The QueryResult represents the result of the Query.

The privacy preservation ontology is created by using Protégé (<https://protege.stanford.edu>) ontology editor. Figure 1 shows the privacy preservation ontology's class hierarchy.

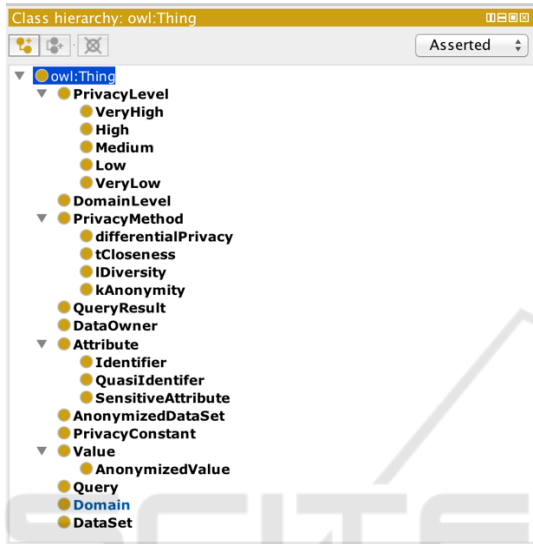


Figure 1: Ontology class hierarchy.

Figure 2 and Figure 3 show the object and data properties, respectively.

Figure 4 shows the graph representation of the ontology. The domain-range relationship of the object properties is given in Table 1.

## 4 A CASE STUDY

The proposed personalized privacy preservation approach is domain independent. Therefore, the main concepts of the approach can be applied to different domains. In this paper, we applied our approach to the health domain. As psychiatry sub-domain is one of the major privacy-concerned field of the health domain, we specifically applied our approach to psychiatry clinic data.

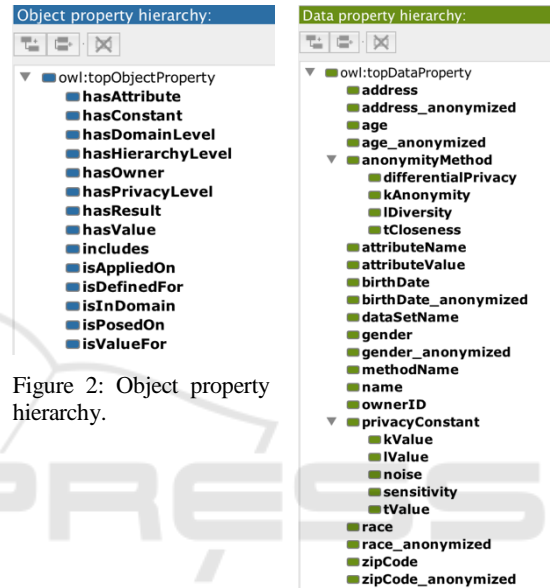


Figure 2: Object property hierarchy.

Figure 3: Data type property hierarchy.

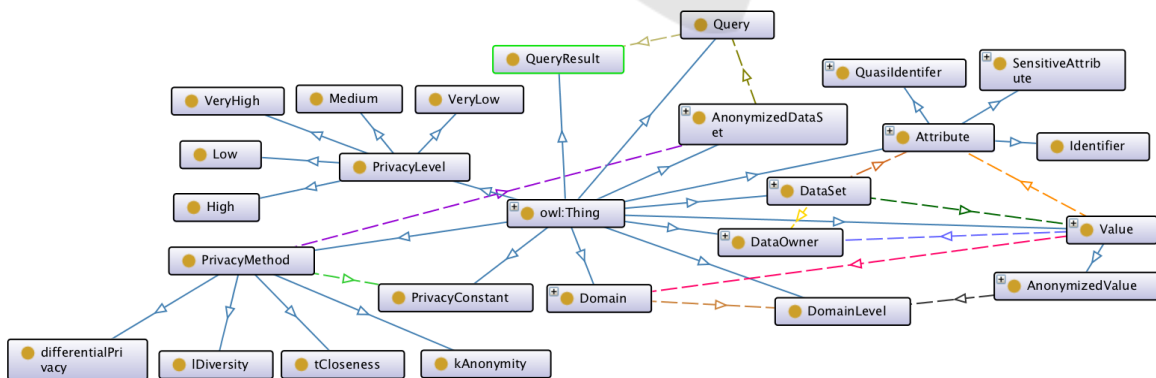


Figure 4: An ontology graph representation for the personalized privacy preservation ontology.

Table 1: Domain and range information for the object properties.

Domain	Property	Range
DataSet	hasAttribute	Attribute
DataSet	includes	DataOwner
DataSet	hasValue	Value
Value	isValueFor	Attribute
Value	hasOwner	DataOwner
Value	isInDomain	Domain
Query	hasResult	QueryResult
PrivacyMethod	isAppliedOn	AnonymizedDataSet
PrivacyMethod	hasConstant	PrivacyConstant
PrivacyLevel	isDefinedFor	DomainLevel
Domain	hasHierarchyLevel	DomainLevel
AnonymizedValue	hasDomainLevel	DomainLevel
AnonymizedValue	hasPrivacyLevel	PrivacyLevel
AnonymizedDataSet	isPosedOn	Query

Table 2: Psychiatry clinic data example.

SSN	Name	Race	Age	Gender	Zip Code	Diagnose
123456789	David Smith	black	38	Male	74142	Schizophrenia
234567891	John Smith	black	55	Male	74142	Alzheimer
345678912	Mary Smith	black	52	Female	74183	Obsessive Compulsive
456789123	Ann Smith	white	17	Female	74183	Obsessive Compulsive
567891234	Jane Smith	black	43	Female	74183	Depression

The psychiatry clinic data include sensitive information on patients’ personal records and health records of psychiatric diagnosis. The disclosure of these data can be very critical and consequently this could adversely affect an individual’s life. Thereby, privacy protection must be ensured to maintain individuals’ trust. Table 2 shows a sample of psychiatry clinic data.

In our case study, PsychiatryClinic represents the DataSet of a psychiatry clinic. We assume that anonymization methods are applied on this data set.

PsychiatryClinic has the following attributes:

- hasAttribute(PsychiatryDataCenter, ZipCode)*
- hasAttribute(PsychiatryDataCenter, Age)*
- hasAttribute(PsychiatryDataCenter, Diagnose)*
- hasAttribute(PsychiatryDataCenter, Gender)*
- hasAttribute(PsychiatryDataCenter, Race)*

John Smith and Mary Smith are two patients who are DataOwner in PsychiatryClinic. Figure 5 shows the property assertions of PsychiatryClinic.

- includes(PsychiatryClinic, Mary\_Smith)*
- includes(PsychiatryClinic, John\_Smith)*

In Table 2, Mary\_Smith’s social security number is “345678912” and her diagnosis is

“Obsessive Compulsive”. In the anonymization ontology, she has Age, Race, Gender, ZipCode and Diagnosis attributes. While Diagnosis attribute is defined as a SensitiveAttribute, the rest of the attributes are defined as “QuasiIdentifier”. The stated definitions are given in the following:

- ValueFor(Mary\_Smith\_Age, Age)*
- isValueFor(Mary\_Smith\_Race, Race)*
- isValueFor(Mary\_Smith\_Gender, Gender)*
- isValueFor(Mary\_Smith\_ZipCode, ZipCode)*
- isValueFor(Mary\_Smith\_Diagnosis, Diagnosis)*
- hasOwner(Mary\_Smith\_Age, Mary\_Smith)*
- hasOwner(Mary\_Smith\_Race, Mary\_Smith)*
- hasOwner(Mary\_Smith\_Gender, Mary\_Smith)*
- hasOwner(Mary\_Smith\_ZipCode, Mary\_Smith)*
- hasOwner(Mary\_Smith\_Diagnosis, Mary\_Smith)*

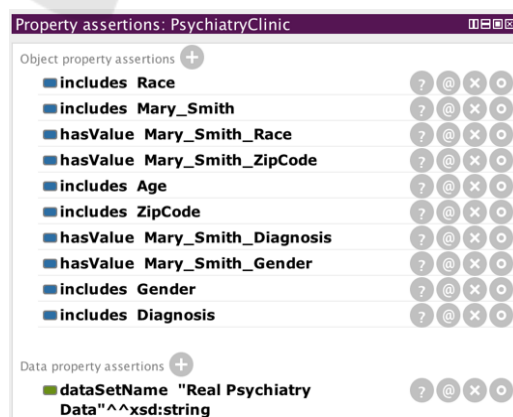


Figure 5: Property assertions of PsychiatryClinic for Mary\_Smith.

In order to provide personalization, data owners must decide the privacy level of their attributes for the anonymization. Figure 6 shows the privacy level for the Gender attribute of *Mary\_Smith*.

Besides choosing the privacy level, the user can also choose which anonymization method will be used on her data. For this purpose, we created two instances: *AnonymizedPsychiatryClinicData* and *AnonymizedPsychiatryClinicData2*. Both data sets are *Mary\_Smith*'s anonymized data sets and different anonymization methods are applied to these data sets which include *Mary\_Smith*'s attributes. Hence, each anonymization method uses different privacy constants, *AnonymizedPsychiatryClinicData* uses *k-anonymity* as *PrivacyMethod* and has a value of 2 as *PrivacyConstant* and *AnonymizedPsychiatryClinicData2* uses *l-diversity* as *PrivacyMethod* and has a value of 3 as *PrivacyConstant*. The specified definitions are stated in the following:

*isAppliedOn(PrivacyMethod\_kAnonymity, AnonymizedPsychiatryClinicData)*  
*hasPrivacyConstant(PrivacyMethod\_kAnonymity, 2)*  
*isAppliedOn(PrivacyMethod\_lDiversity, AnonymizedPsychiatryClinicData2)*  
*hasPrivacyConstant(PrivacyMethod\_lDiversity, 3)*

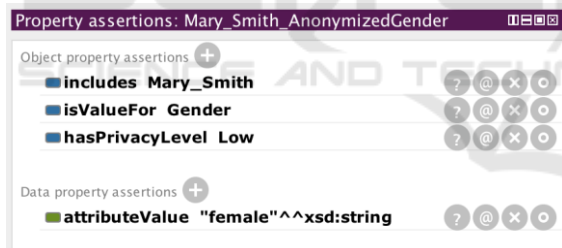


Figure 6: Privacy level for *Mary\_Smith*'s Gender attribute.

Figure 7 and Figure 8 show the property assertions of *AnonymizedPsychiatryClinicData* and *AnonymizedPsychiatryClinicData2*, respectively.

## 5 QUERYING PERSONALIZED PRIVACY ONTOLOGY

After generating the personalized privacy ontology, SPARQL (<http://www.w3.org/TR/rdf-sparql-query>) queries are executed on the proposed ontology. In Figure 9, a query and its results are shown. The query lists all data sets that any anonymization technique is

applied on. The query result shows anonymized data sets, privacy methods and privacy method's constants. The second query, shown in Figure 10, lists the anonymized values of data sets, their privacy levels that are determined by individuals, and the privacy method used for anonymization.

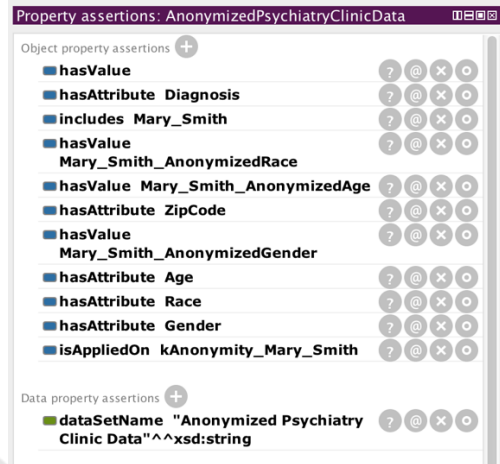


Figure 7: Property assertions of *AnonymizedPsychiatryClinicData*.

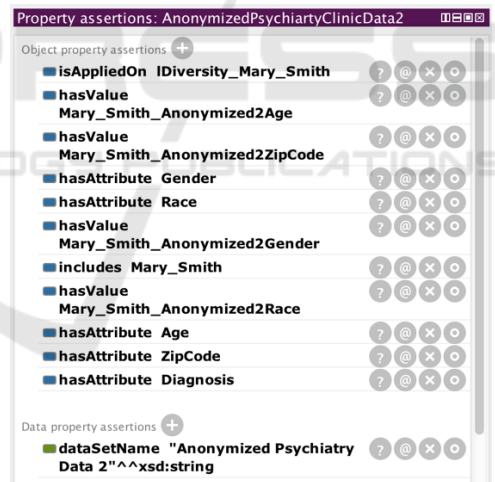


Figure 8: Property assertions of *AnonymizedPsychiatryClinicData2*.

## 6 CONCLUSIONS

The proposed ontology based personalized privacy preservation model is a domain independent model and aims to preserve privacy by using data anonymization methods within a Semantic Web environment.

```
SPARQL query:
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX ao: <http://www.semanticweb.org/oc/ontologies/2015/AnonymityOntology#>

SELECT ?anonymizedDataSet ?privacyMethod ?privacyMethodConstant ?privacyConstant
WHERE {
  ?anonymizedDataSet ao:usePrivacyMethod ?privacyMethod.
  ?privacyMethodConstant ao:hasPrivacyConstant ?privacyConstant.
  ?anonymizedDataSet ao:isAnonymized ?true.}

anonymizedDataSet | privacyMethod | privacyMethodConstant | privacyConstant
AnonymizedPsychiatryClinicData | "kAnonymity"@ | IDiversity_Mary_Smith | "3"^^<http://www.w3.org/2001/XMLSchema#integer>
AnonymizedPsychiatryClinicData2 | "IDiversity"@ | IDiversity_Mary_Smith | "3"^^<http://www.w3.org/2001/XMLSchema#integer>
AnonymizedPsychiatryClinicData | "kAnonymity"@ | kAnonymity_Mary_Smith | "2"^^<http://www.w3.org/2001/XMLSchema#integer>
AnonymizedPsychiatryClinicData2 | "IDiversity"@ | kAnonymity_Mary_Smith | "2"^^<http://www.w3.org/2001/XMLSchema#integer>
```

Figure 9: A query listing all anonymized data sets with their privacy methods.

```
SPARQL query:
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX ao: <http://www.semanticweb.org/oc/ontologies/2015/AnonymityOntology#>

SELECT ?anonymizedValue ?privacyLevel ?privacyMethod
WHERE {
  ?anonymizedValue ao:hasPrivacyLevel ?privacyLevel.
  ?anonymizedValue ao:usePrivacyMethod ?privacyMethod}
```

anonymizedValue	privacyLevel	privacyMethod
Mary_Smith_AnonymizedPsychiatryClinicData_Gender	"Low"@	"kAnonymity"@
Mary_Smith_AnonymizedPsychiatryClinicData_Race	"Low"@	"kAnonymity"@
Mary_Smith_AnonymizedPsychiatryClinicData_Age	"Medium"@	"kAnonymity"@
Mary_Smith_AnonymizedPsychiatryClinicData2_ZipCode	"Medium"@	"IDiversity"@
Mary_Smith_AnonymizedPsychiatryClinicData2_Race	"Medium"@	"IDiversity"@
Mary_Smith_AnonymizedPsychiatryClinicData2_Age	"Medium"@	"IDiversity"@
Mary_Smith_AnonymizedPsychiatryClinicData2_Gender	"High"@	"IDiversity"@
Mary_Smith_AnonymizedPsychiatryClinicData_ZipCode	"Medium"@	"kAnonymity"@

Figure 10: A query listing anonymized values with their privacy levels and methods.

The proposed model is data and domain independent. Therefore, the model can be applied to different forms of data and also to different domains. As users may have different privacy preferences, the proposed privacy model supports a personalized approach. In order to apply personalized privacy preservation, individuals’ personal privacy preferences are taken into consideration in the proposed model.

As a future work, we will add a purpose-based approach to the personalized privacy concept of the model. Purpose based privacy will strengthen the customization of individuals’ privacy preferences and maximize the quality of data analysis. Also, a framework based on the proposed privacy preserving ontology model will be developed by using Apache Jena (<https://jena.apache.org>). The framework will suggest a privacy preserving algorithm depending on

privacy levels of attributes. The framework will be evaluated for psychiatry data in the healthcare domain. Also, the model will be examined for different personalized privacy levels and the quality of the query results will be evaluated based on the used anonymization method.

## REFERENCES

Ayala-Rivera, V., et al. 2017. Enhancing the Utility of Anonymized Data by Improving the Quality of Generalization Hierarchies. *Transactions On Data Privacy*, 10 (2017):27–59.

Can, O. 2018. Personalized Anonymity for Microdata Release. *IET Information Security*. 12(4): 341-347.

Ciriani, V., De Capitani di Vimercati, S., Foresti, S., Samarati, P.. 2007. k-Anonymity. *Secure Data*

- Management in Decentralized Systems (Advances in Information Security)*, Springer, US, 1<sup>st</sup> edition, pp. 323-353
- Dwork, C. 2008. Differential Privacy: A Survey of Results. In *International Conference on Theory and Applications of Models of Computation*. Vol. 4978, pp. 1-19.
- Dwork, C., Roth, A. 2014. The Algorithmic Foundations of Differential Privacy. *Theoretical Computer Science*. Vol. 9, Nos. 3–4, pp. 211–407.
- Gedik, B., Liu, L. 2008. Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms. *IEEE Transactions on Mobile Computing*. 7(1): 1-18
- Kenig, B., Tassa, T. 2012. A Practical Approximation Algorithm for Optimal k-Anonymity. *Data Mining and Knowledge Discovery*. 25(1):134-168.
- Kern, M. 2013. Anonymity: A Formalization of Privacy-l-Diversity. *Seminars Future Internet/IITM/ACN SS2013, Network Architectures and Services*. pp. 49-56.
- Li, N., Li, T., Venkatasubramanian, S. 2007. t-Closeness: Privacy Beyond k-Anonymity and l-Diversity. In *IEEE 23rd International Conference on Data Engineering 2007 (ICDE Conference 2007)*. IEEE.
- Machanavajjhala, A., Gehrke, J., Kifer, D., Venkatasubramanian, M. 2006. l-Diversity: Privacy Beyond k-Anonymity. In *22nd International Conference on Data Engineering (ICDE'06)*. IEEE.
- Martínez, S., Sánchez, D., Valls, A. 2010. Ontology-Based Anonymization of Categorical Values. In *International Conference on Modeling Decisions for Artificial Intelligence*, Vol. 6408, pp. 243-254. LNCS, Springer.
- McCallister E, Grance T, Scarfone K. 2010. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) Rep. *NIST Special Publication 800-122*. 58pp
- Mendes, R., Vilela, JP. 2017. Privacy-Preserving Data Mining: Methods, Metrics, and Applications. *IEEE Access*. 5: 10562-10582.
- Miracle, J., Cheatham, M. 2016. Semantic Web Enabled Record Linkage Attacks on Anonymized Data. In *Proceedings of the 4th Workshop on Society, Privacy and the Semantic Web - Policy and Technology (PrivOn2016) in 15th International Semantic Web Conference*. CEUR.
- Omran, E. et al. 2009. A K-anonymity Based Semantic Model for Protecting Personal Information and Privacy'. In *IEEE International Advance Computing Conference 2009 (IACC 2009)*, pp. 1443-1447. IEEE.
- Project HealthDesign. 2009. The Need to Know: Addressing Concerns About Privacy and Personal Health Records. *Reports from Round 1*.
- Ruggieri, S. 2014. Using t-closeness anonymity to control for non-discrimination. *Transactions On Data Privacy*. 7(2014): 99–129.
- Sarathy, R., Muralidhar, K. 2011. Evaluating Laplace Noise Addition to Satisfy Differential Privacy for Numeric Data. *Transactions on Data Privacy*. 4(1): 1-17.
- Soria-Comas, J., Domingo-Ferrer, J. 2013. Connecting privacy models: synergies between k-anonymity, t-closeness and differential privacy. In *Conference Of European Statisticians*. EUROSTAT.
- Sweeney, L. 2002. k-Anonymity: A model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*. 10(5): 557-570.
- Usenmez, B., Can, O. 2015. Conceptualization of Personalized Privacy Preserving Algorithms. In *9th Int. Conf. on Metadata and Semantics Research Conference*. Vol. 544, pp. 195-200. Springer.
- Wong, R., Li, J., Fu, A., Wang, K. 2006. ( $\alpha$ , k)-Anonymity: An Enhanced k-Anonymity Model for Privacy-Preserving Data Publishing. In *Proc. of the 12th ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining*, pp. 754-759. ACM.
- Xiao, X., Tao, Y. 2006. Personalized Privacy Preservation'. In *Proc. of the 2006 ACM SIGMOD Int. Conf. on Management of data*, pp. 229-240. ACM.