Control Algorithm to The Semantic Data Security in Computer Networks

KHALED SADEQ AL-SHREDEI, MOHAMAD A. A. AL-RABABAH and NOUR E. OWEIS

King AbdulAziz University, Northern Border University, Jeddah, Saudi Arabia
Technical University of Ostrava, Faculty of Electrical Engineering and
Computer Science, Arar, Saudi Arabia

ABSTRACT

In this paper we will talk about information technology semantic , which plays an important role in many areas of human activity and therefore the task of data security semantic is very important for information technology and will consider this research to support the idea of data semantic cards safety of RDF tri- called safety data. Also with the security of confidential data labels in different security levels in different departments have different ranges and variety of use of user data. There are ongoing contacts with the idea of safety data on the labels of three diverse In this research has identified the main rules to control user access to the data by comparing the levels of access to the user (the security levels triple) Based on these rules and advanced algorithms will do read and modify data RDF triple.

Key words: Data security, Computer networks, Information technology.

INTRODUCTION

We will discuss here the right of the user to access the data that will keep the data confidential for various reasons, such as: Plans things personal and private, and the campaign, military information, or government plans if there is not an effective way to ensure data security, it may be the user and unauthorized access to the data and take drastic measures for the database . Therefore, the task of creating the control of user access rights is relevant.

We will discuss here the right of the user to access the data that will keep the data confidential for various reasons, such as: Plans things personal and private, and the campaign, military information, or government plans if there is not an effective way to ensure data security, it may be the user and unauthorized access to the data and take drastic measures for the database . Therefore, the task of creating the control of user access rights is relevant.

Solve the problem of semantic technology, is a way to control access to data with security labels for each RDF triple - so - called data. This method of controlling access to RDF data - compared with triangles triplets security labels of user rights.

1.   To filter results according to a whole sub tree (e.g., if a user selects 'ontologies' in a facet based on the categories in Fig. 1, all objects about 'OWL' and 'Ontology Reasons' can be automatically included in the result set, too).

2.   To find communities (e.g., for a query 'XML', the facet might show a large number of objects in 'RDF' and in 'OWL', but not in 'Rules').

3. To characterize authors or groups of authors (e.g., showing that the objects authored By a particular person are mainly about the topics 'OWL' and 'Rules').
4. To characterize the object collection as a whole (e.g., if a query 'rules' only provides Results related to 'Semantic Web', but not about 'business rules').

Safety components for triplet RDF-data

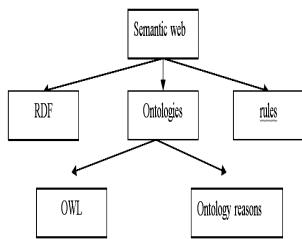Typically, the resource belongs to the triplet

Fig. 1: Example categorization system for topics

the resource. In this case, the sensitive label sls, associated with the resource should have the following characteristics:
1. slt is minimum sensitivity label for any triplet using the resource as a subject . In other words, the sensitive label slt for the triplet should cover the mark for the subject sls, where stt ≥ sls;
2 . stew label for the newly added triplet is initialized by the user only if it is dominated by the label associated with the subject of the triplet , then sltnew ≥ sls;
3 . Only a user with an affordable tag stuser, the dominant label of the subject and of the triplet, triplet can read , then stuser ≥ slt and stuser ≥ sls .

Default sls medium occurs by use when RDF resource is taken as the initial subject triplet time. Sensitive default label in this case is set in the initial user triplet sensitive label. Sensitive default label is a label which is inserted by the user for all triplets. To check the security labels triplets SL = {sl1, sl2,, sln} and adding a new triplet Tnew, in which a subject S has a label security, algorithm. This use case shows how to find the graph for the keyword 'RDF' for the Period 2001–2005. The description follows the three main parts of the

state of the object can be described by the use of additional claims RDF. Resource RDF, which is in the object position of the triplet, may appear in the position of the subject of another triplet. Then, if the resource is in the position of the object does not have the sensitive label, the label associated with the resource in the position of the subject is the default label for the object[2] .

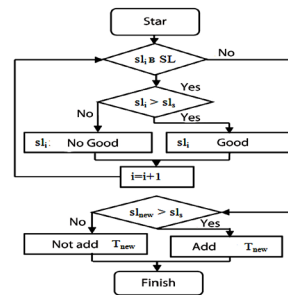The resource appears in the role of the subject triplet, where a statement is made about

Fig. 2: The algorithm for adding a new triplet

algorithm to
(1)   create a co-occurrence matrix including higher order co-occurrences
(2)   Find relations between keywords.
(3)   Create a graph for the keyword 'RDF'. In out demonstrator,
(4)   4 all graphs are periodically updated (so the version in the Web might differ from the graphs presented here).

Top-X and Biased Page Rank After creating the co-occurrence matrix M, the Algorithm first extracts the corresponding 'RDF' row of M, comprising the weighted Co-occurrences of 'RDF' (using the ICF as weight) with all other keywords. This matrix Row is sorted according to the matrix values (cf. left part of Table 1; the plain Co-occurrence values are shown for comparison in this example, the direct neighbors of 'RDF' are 'RDF' itself (the start keyword is Included by definition), 'Semantic Web' and 'Metadata' as they accumulate P = 20% Of the total sum of matrix values of all keywords in that list.
1.   Afterwards, the algorithm uses Page Rank (biasing to 100% on the three direct keywords Of 'RDF') to find a new ranking. The resulting Page Rank score vector includes
2.   Higher-order co-occurrences, which are

Table 1: Direct neighbors (left) / the Page Rank score vector (right) for 'RDF' (top-X = 5)

rank	keyword	m (j, i)	cook (i, j)
1	RDF	259.8	55
2	Semantic Web	112.1	31
3	Metadata	55.3	15
4	XML	41.4	15
5	Annotation	26.3	6
6	Ontology	26.1	8
7	DAML	23.1	4
8	RDF Schema	20.6	3
9	DAML+OIL	18.0	3
10	OWL	16.0	3
rank	keyword	score	
1	Semantic Web	828.1	
2	Metadata	755.0	
3	RDF	746.4	
4	Ontology	127.1	
5	XML	120.2	
6	Web Service	74.6	
7	Information Retrieval	50.2	
8	Data Mining	49.3	
9	Clustering	49.3	
10	Annotation	49.0	

Table 2: Page Rank score vectors for 'Semantic Web' (left;X = 10) & 'Metadata' (right;X = 18)

Rank	Keyword	Score
1	Semantic Web	407.7
2	Ontology	373.0
3	XML	358.4
4	Web service	330.6
5	RDF	311.4
6	metadata	303.5
7	Description Logics	288.5
8	OWL	284.3
9	Data Mining	47.8
10	security	45.6
Rank	Keyword	Score
1	Metadata	262.6
2	XML	125.1
3	Semantic Web	207.1
4	Digital Libraries	199.5
5	Ontology	197.5
6	Interoperability	172.3
7	Annotation	171.8
8	RDF	167.1
9	WEb	151.1
10	OAI	149.7

not reflected in the sorted co-occurrence vector.

3. Practically speaking, the main objective of the first part is to see whether the start Keyword 'RDF' itself remains the 'top keyword' in the score vector after running the Biased Page Rank or if other keywords are more relevant and 'overtake' (in the sorted Co-occurrence vector, the start keyword stays always on top). As shown in the right part Of Table 1, indeed 'Semantic Web' and 'Metadata' achieve a higher score than 'RDF'

4. And are candidates for subsuming 'RDF.

5. Deriving Relations the basic idea of the second part to identify 'consumption'

Relations between 'RDF' and its direct neighbors is to do a pair wise comparison of the Scores of two vectors: the Page Rank score vector of 'RDF' and of its direct neighbors for the direct neighbor 'Semantic Web', the score of 'RDF' is lower than the score of 'Semantic Web' in both the Page Rank list of 'Semantic Web' (cf. Table 2 (left)) and the Page Rank list of 'RDF' (cf. Table 1 (right)). Hence,

'RDF' is defined to be Subsumed by 'Semantic Web' (RDF achieves a sufficiently high score in both lists not to be affected by tail cutting). Since 'RDF' is among the top-X = 8 elements of the Page Rank score vector of 'Semantic Web', the confidence in this relation is defined as 'Strong'. Analogously, 'RDF' is found to be subsumed by 'Metadata'.

Connotations and found names with spaces in applications and uses

RDF about My Apartment

Let taubz: abbreviate http://razor.occams.info/index.html#

Taubz:me http://example.org/own taubz:my_apartment

taubz:my_apartment http://example.org/has taubz:my_computer

taubz:my_apartment http://example.org/has taubz:my_bed

taubz:my_apartment http://example.org/is_in http://example.org/Philadelphia

So far, I have shown how RDF can be used to describe the relationships between entities in the

world. RDF can be used reliably and high quality also, to see the predicates RDF documents as the applications which have been. The conclusion to this paper shows us a lot of things that benefit us, such as the audit phase of the data and the available topics and data and ensure continued quality and source of issuance and to any face as this application give concrete names in the global real-world of resources. Ontologies, schemas, and vocabularies, which all mean roughly the same thing, are RDF information about... other RDF information.

To be upgraded significantly RDF and make sure the proper official documents and all high reliability and confidentiality to raise the quality of XML in order to identify the XML schemas. But as different as they are the same. XML with all the reliability to be applied and utilized as useful applications and uses in any of the RDF, which itself is written in RDF, and the provision of relations between there are many things that Results ,

RESULTS

RDF- data are essential elements of the semantic data . For safety semantic database, RDF- secures data. These papers discussed the main elements of the RDF- data. The algorithms for determining the security labels triplet, as well as to check the access rights of users to triplets .

In RDF- data resource can have different roles (subject, predicate , object) in a variety of triplets. Because of this, the security label of triplets, made for a particular type of resource depends on its security labels . To check the security labels triplets algorithm.

REFERENCES

1. Martin Bravenboer and Eelco Visser. Concrete syntax for objects :domain-specific language embedding and assimilation with out restrictions. In Proceedings of the ACM SIGPLAN Conference on Object-oriented Programming, Systems, Languages, and Applications (OOPSLA), 2004.

2. Kathleen Fisher, David Walker, Kenny Q. Zhu, and Peter White. From dirt to shovels: Fully automatic tool generation from ad hoc data. In ACM Symposium on Principles of Programming Languages, 421–434 (2008).

3. Wilkinson, K., Sayers, C., Kuno, H., Reynolds, D.: Efficient RDF Storage and Retrieval in Jena2. In: Proceedings of First International Workshop on Semantic Web and Databases 131–150 (2003).

4. Bizer, C.: RAP (RDF API for PHP). Website http://www.wiwiss.fuberlin. de/suhl/bizer/rdfapi/ (2004).

5. Beckett, D.: The design and implementation of the Redland RDF application Framework. Computer Networks **39**: 577–588 (2002).

6. Bizer, C., Seaborne, A.: D2RQ -Treating Non-RDF Databases as Virtual RDF Graphs. Poster (2004) 3rd International Semantic Web Conference (ISWC2004), Hiroshima, Japan.

7. Dietzold, S.: Generating RDF Models from LDAP Directories. In Auer, S., Bizer, C., Miller, L., eds.: Proceedings of the SFSW 05 Workshop on Scripting for the Semantic Web , Hersonissos, Crete, Greece, May 30, 2005. Volume 135 of CEUR Workshop Proceedings., CEUR-WS (2005).

8. Prud'hommeaux, E., Seaborne, A.: SPARQL Query Language for RDF (Working Draft). W3c working draft, World Wide Web Consortium (W3C) (2006)

9. Seaborne, A.: RDQL - A Query Language for RDF. W3c member submission, World Wide Web Consortium (W3C) (2004) http://www.w3.org/Submission/2004/SUBM-RDQL-20040109/.

10. Reddivari, P., Finin, T., Joshi, A.: Policy based access control for an RDF store. In Kagal, L., Finin, T., Hendler, J., eds.: Policy Management for the Web. 78–81 (2005).

11. Dietzold, S.: LACS: Lightweight Access Control Schema. OWL ontology (2006) http://purl.org/net/lacs.

12. R. Sandhu, E. J. Coyne, H. Feinstein. Role-based access control models // IEEE Computer. – **29**(2): P. 38–47 (1996.)

13. P. Stachour and B. Thuraisingham. Design of LDV: A multilevel secure relational database management system // IEEE Trans. Knowledge and Data Eng. **2**(2): 190–209 (1990) .