Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

December 2014, pg.06 – 11

NATIONAL CONFERENCE ON ADVANCES IN MODERN COMPUTING AND APPLICATION TRENDS
TECHMAN-14
5th & 6th December, 2014, Organized by Acharya Institute of Technology, Bangalore, India

Policy Reasoner: An Approach for Security to RDF

C.Viswasanathan[1], Dr. Deepti A.R[2]

[1-2]Department of MCA, Acharya Institute of Technology, India

Abstract— This paper focuses on the security methods for Resource Description Framework (RDF). The open nature of the semantic web hinges on the seamless autonomous interoperable communications among unknown entities and formats. This envisioned semantic web is expected to raise new security concerns. This paper presents the survey of existing work on security methods at the basic level of RDF for semantic web integration. Through this survey we found that most of the security measures are specified using access control policies for triple referencing and inference protection. For the later, there is least research work initiated. Thus, in this paper, we propose a Policy-Reasoner for RDF, a combination of access specification as well, a reasoning engine, which address the security issues at large in RDF triples level.

I. INTRODUCTION

The rapid development of the World Wide Web has led to the development of machine understandable, self describing syntax to exchange information. To support these web based applications, semantic web community propose many semantic model, in that one such model is the Resource Description Framework (RDF) [2] which is supported by the WWW consortium [22]. The success of RDF and the semantic web will depend on the 1. Development of applications that prove the applicability of the semantic vision concept. 2. The information users' confidence about the privacy and security of such information accessible over semantic web. 3. Availability of interfaces and tools to enable the development and deployment of such applications. 4. Semantic data stores and inference system that exploit RDF to identify and locate the most relevant web resources. In addition, many practical issues such as sensitivity of information accessible on semantic web and the security related compatibility for general use will be crucial to the success of RDF. This paper discusses the preliminary investigation on enforcement security aspects at Semantic Web. In particular, we provide an overview of security consideration by focusing our research at RDF level towards a policy framework.

The organization of this paper is as follows. Section 2 provides some background information on RDF. Section 3 surveys related work and discuss the various aspects of RDF security. Section 4 shows how the proposed method called, Policy-Reasoner for RDF can be used for the specification and enforcement of access control policies. Section 5, concludes by outlining the future directions of RDF and semantic web.

II. BACKGROUND ON RDF

Resource Description Framework (RDF) has established a widely used standard for representing data in the Semantic Web. Several commercial and academic efforts target the development of RDF datasets. The popularity of the RDF data model [2] and the RDF Schema language is due to the flexible and extensible representation of information under the form of triples. The three components of RDF are resources, properties and statements like a web page, a property, or specific attribute as data source. A sample RDF document and its description are given below in a graph format in Fig.1.1

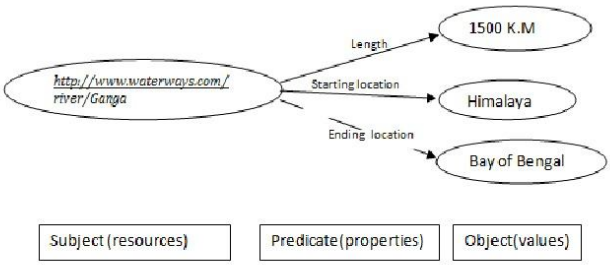

Fig.1.1 RDF Graph

RDF graphs are generated to represent statements for the given relation of a triple set. RDF statements can be serialized using XML to document the data and attribute sets as shown in fig.1.2. RDF provides better support for interoperability as well as searching, cataloguing and referencing. SPARQL [8] is a W3C supported standard query language for querying the RDF stores.

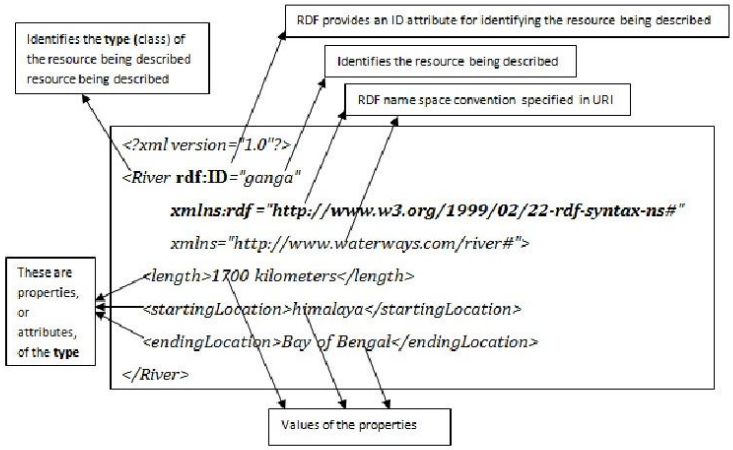

Fig:1.2 XML serialized RDF

III. RDF SECURITY

Traditional security methods for semantically derived knowledge base cannot ensure the various security issues such as, authentication, authorization, confidentiality, privacy, reputation and exposure control etc., So, there is a need for security mechanisms to secure RDF and their relationships from unauthorized access and misinterpretations. This plays a vital role beyond the usual encryptions, firewalls and password based methods to make the semantic web reliable. As security is involved among several layers of semantic web starting from the transmission protocols to trust during the semantic web information exchange, RDF faces many challenging in the security issues which denoted in fig1.3.

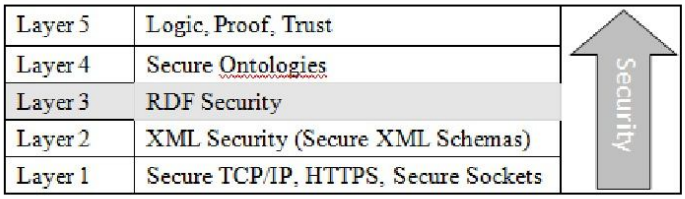

Fig 1.3 Security Layers in the Semantic Web

Therefore, RDF model is the key to the integration of meaningful singular database from heterogeneous resources; our focus is to secure the data at RDF layer.

IV. RELATED WORK

Flouris et. al [10]provide a fine grained access control framework on top of RDF repositories including high level specification language. In their work, they give the specification of permissions for update operations, access control permissions on set of RDF triples for fine-grained access control. To express such access control permissions, they use the notion of triple patterns from the SPARQL[7] language. Role Based Access Control (RBAC) [5] [23] method establishes relations between users-roles-permissions. It is difficult to change the access right of entities without changing the role of the concerned entities. This limits the application because of close coupling of roles and access rights. Carminati, Ferrari and Thuraibgham [4] proposed a security framework that uses RDF for policy specification and enforcement. The framework utilizes the semantic richness of RDF for expressing security information by making policy specification. The Platform for Privacy Preferences (P3P) is a standard [1][3] developed by the W3C that enables websites to describe the users privacy policies and allows browsers to decide whether they match the users preferences. This work improves the security of hiding the user's personal information. Rei (Rei Policy Language) [16] is a policy specification language over a domain for user specified privacy. It allows specification of declarative policies over domain ontologies in RDF, DAML+OIL and OWL[12]. It details its usage for user privacy preference specification as an enhanced web privacy framework. F.Abel et.al [8] propose specification language using graph patterns, in which policy permissions are injected in the query to restrict the triples accessibility. S. Dietzold et.al [6] gives the requirements for access control language in the context of Semantic Wiki application. O. Sacco and Passant [14] present the PPO vocabulary, expressing access control policies for RDF documents. P. Reddivari et. al [17] presents an access control specification language for defining permission for update operations on RDF data. Most of the access control policies [11][18] to semantic web are specification of rules, filters and complex algorithmic logics to allow or disallow access to information over the distributed web. Our proposed work attempts to establish a framework to protect rightful inferencing along with the specification control.

V. POLICY REASONER – A PROPOSED METHOD

The proposed method namely a Policy – Reasoner fig1.4, is a framework to define explicit rules, query and deference filters work for the prohibition of irrelevant deducing. The whole framework consists of two parts,

Policy Engine: The first part of the framework use SPARQL, a query language of RDF triple and a policy set of specifications, which can apply subset selection query filters to a given entity. The specification of access policy is imparted by inserting additional child nodes in the RDF properties.

1. Policy Reasoner : The second part of the framework envisages a rule processor, which is used to decide the basic synonymous applicability of dereferencing. This would describe a basic vocabulary to store synonyms and rule schemas for the resources.

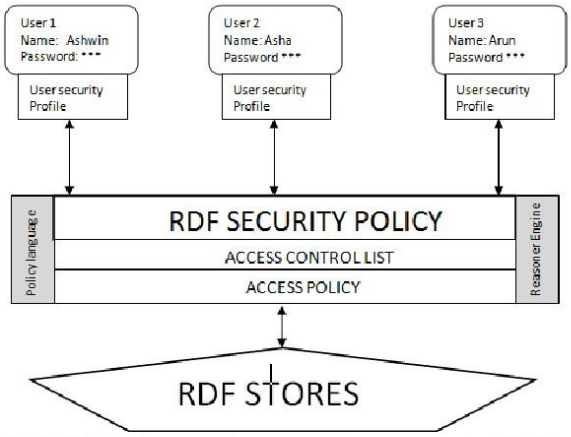

Fig.1.4 A Model Architecture for Security Policy Reasoner for RDF Graph

At the core of the Policy-Reasoner Framework lie the notions of semantic real world synonyms and access control permissions and access policy. Intuitively access control permission is used to explicitly set certain triples in an RDF graph to be accessible or inaccessible. Thus, the proposed framework namely, the Policy – Reasoner not only specifies constraints but attempts security solutions for safe inferred triple. A sample policy specification ontology is given for policy reasoner is given below,

VI. ILLUSTRATION

xmlns per : http://rdf-today.org/xmlns/permissions# (xml name space associated with an URL permission convention)

class: per owl:distinctMembers per:read, per:write, per:create, per:update, per:delete, per:purge, per:clone, per:list .

xmlns domain : http://rdf-today.org/domains#

xmlns resource : http://rdf-today.org/resource#

For simplicity, permissions shown in shorthand notation N3[2] for a set of resources with a set of assertions;

resource : rsource1 per : read domains : domain1, domain : domain2, domain : domain3
Per : create domain: domain1, domain : domain3
Per : update domain: domain 1
Per : noread domain : domain4
per : nocreate domain : doamin4
Per : noupdate domain : domain5

user : user1 per : read resource : r1 establishes that the given user has read relationship on a resource r1.. This relationship also should be declared in the permissions class.

Role : role1 per : read resource : r2 establishes that for a given role, a resource r2 can be read by anyone with the role. Having established the roles, we can use SPARQL ask query to determine whether a given user's role include the appropriate permission to read a given resource.

```
ASK WHERE {
        user : user1 rdf: type ?role .
      resource : r1 rdf : type ?resourceType .
      ?role per:read ?resourceType .
      }
```

If the result of this query is true, then the designated user has the right to read the given resource having the role given permission.

VII. FUTURE DIRECTIONS

There are several access control mechanisms, such as annotation models, security objects embedded in RDF as quadruples, Access Control List by W3C,[22][13] and Role based access control[3] etc. Most of the research for RDF security models, discusses the policy specifications for secure semantic web languages. The proposed study found that no work or least work is initiated for inference control in the semantic web. Based on policy specification, our future work would focus on building working model to include policy specific reasoner with inference control as given in the above architecture which would be an RDF level implementation.

VIII. CONCLUSION

The semantic web is often described as a "web of data" in which information and knowledge is instructed in ways that are easy for machines to process and make use of it. To do this, RDF is explored along with its security aspects and its policy. This paper, establishes the access control specification is one method predominantly used for applying filters in the semantic web for security concerns. Finally, we propose a model, Policy- Reasoner that would combine the policy languages and a reasoner for inference control for appropriate access. Finally, both RDF and semantic web have a long way to go. At this stage, this survey paper shows most of the work are at their intial phases. Solutions to security issues, ease of use and compatibility will be crucial in the success of RDF. The conclusion drawn from the above is that the future of RDF is bright and its research and development opportunities are abundant and useful to many application areas like web mining, e-commerce and e-business etc.

References

[1] Azadeh Nematzadeh, Layla Pournajaf, "Privacy Concerns of Semantic Web". 5th International Conference on Information Technology: New Generations, 2008 IEEE
[2] Berners-Lee. "Notation 3 (N3)" http://www.w3.org/DesignIssues/Notation3/,
[3] http://www.w3.org/TR/2002/WD-rdf-schema-20020430/, April 30, 2002
[4] Cranor, L., Langheinrich, M., Marchiori, M. Presler-Marhshall, M., Reagale. "Platform for Privacy Prefernces (P3P)", 2002
[5] Carminati, B., E. Ferrari and B. Thuraisingham. "Using RDF for policy specification and enforcement". In 15th International workshop on database and expert systems Applications,Los Alamitos,CA,USA,IEEE Computer Society (2004).
[6] D. Ferraiolo and R. Kuhn. "Role-based access controls". In 15th NIST-NCSC National Computer SecurityConference, pages 554563, 1992.
[7] Dietzold and S. Auer. "Access Control on RDF Triple Store from Semantic Wiki Perspective". In ESWC Workshop on Scripting for the Semantic Web, 2006
[8] E. Prud`hommeaux and A. Seaborne. "SPARQL Query language for RDF". www.w3.org/TR/rdf-sparql-query, January 2008
[9] F. Abel, J.L De Coi, N. Henze, A. Wolf Kosling , D. Krause , D. Olmedilla. "Enabling Advanced Context-Dependant Access Control Policy in RDF stores". In ISWC/ASWC, 2007
[10] Carminati, B., et al. "Security for RDF". Proceedings of the DEXA Conference. Workshop on Web Semantics, Zaragoza, Spain, 2004.
[11] G. Flouris, I. Fundulaki. M. Michou ad G. Antoniou. "Controlling Access to RDF Graphs". In Proceedings of FIS - pages 107 – 117, 2010
[12] Javanmardi, S., Amini, M., Jalili, R., GanjiSa_ar, Y. "SBAC:A SemanticBased Access Control Model". In: 11th NordicWorkshop on Secure IT-systems (NordSec'06), Linkping, Sweden. (2006)
[13] Mike Dean and Guus Schreiber. "OWL web ontology language reference", 2004
[14] OASIS (Organization for the Advancement of Structured Information Standards). Oasis Web Site: http://www.oasis-open.org/
[15] O. Sacco, A. Passant, S. Decker, "An access control Framework for the web of Data. In proceedings of Trustom, IEEE, page 456-463, 2011
[16] Ora Lassila and Ralph R. Swick, "Resource Description Framework (RDF) Model and Syntax Specification", Technical Report, W3C Recommendation, 1999., http://www.W3.org/, www.w3.org/TR/rdf-primer
[17] Lalana Kagal. "A Policy-Based Approach to Governing Autonomous Behaviour in Distributed Environments". PhD thesis, University of Maryland Baltimore County
[18] Reddivari, T. Finn, A. Joshi. "A policy based Access control for RDF store". In Semantic Wb for Collaborative Knowledge Acquisition ,2007.
[19] Sabrina Kirrane, "Knowledge Based Access Control Policy Specification and Enforcement", DC Proposal at Digital Enterprise Research Institute

[20] T. W. Finin, A. Joshi, L. Kagal, J.Niu, R.S Sandhu, W.H Winsborough and B.M Thuraisingham. "ROWLBAC: Representing role based access controlin OWL", In proceedings of SACMAT, pages 73-82, 2008.
[21] Tim Berners Lee, James Hendler and Ora Lessila,"The Semantic Web", Scientific American, 284(5):34-43, 2001Thuraisingham, B. "Security Standards for the Semantic Web". Computer Standards and Interfaces 27, 2005, pp 257-26
[22] W3C (World Wide Web Consortium). W3C Web Site: http://www.w3.org/Yialelis, N Lupu. E. Sloman, M: "Role Based security for distributed systems"(1996).

