Secure Semantic Web Application Using Dynamic Sparql Queries

Sincy Abraham[1], Jyolsna Mary.P[2]
[1]Dept of Computer Science & Engineering
[2]Assistant Professor, Dept of Computer Science & Engineering
[1, 2] MBCCET Peermade - 685531, Idukki, Kerala, India

Abstract- *Semantic web is a significant advancement of internet technology. The world of data is linked together is called Sematic Web. Many of the people are accessing a web. So security of database become challenges. Several studies have discussed the security of the Semantic Web at various layers. Limited number of researchers have studied the database security. Here investigate the various database security issues Sematic Web application. And provide security robustness using dynamic SPARQL queries. Various Access control mechanism and applying hashing algorithm for attack prevention. These techniques are used to provide high secure semantic web and this encourages to developers to move towards semantic web technology.*

Keywords- CSTR-PID-ZN-Fuzzy-MRAM-MATLAB.

I. INTRODUCTION

The Semantic Web is an extension of the World Wide Web through standards by the World Wide Web Consortium. Web 1.0 referred as a first stage of world wide web, which is entirely made of webpages connected by Hyperlink. It provides a static website and not provide a interactive content. Web 2.0 is the second stage development of internet technology; it changes from static web pages to dynamic webpages. Web3.0 semantic web is a recent innovation of the internet technology. These standards promote common data formats and exchange protocols on the Web, most fundamentally the Resource Description Framework. In 2013 more than four million web domains contained semantic web mark up. Peoples companies' researchers, universities etc. are using internet and it provide chances of various type of cyber-attacks [8][9]. Today several systems have started moving their data to be linked on the world of data. So security of semantic web is challenges.

Several studies discussed the security of the semantic web in different layers. But some number of researches only concentrate on data base security like SPARQL injection attacks [1][3][4]. They are applied their test using java and RDF data is placed on Jana frame work. But these work not provide sufficient security in database. Because they provide only static system. And they are not using PHP as development languages.

II. CONCEPT OF SEMANTIC WEB AND SPARQL

Semantic web uses a standardized graph data model namely RDF Recourse Description Frame Work to make its a machine readable. Semantic web are collection of RDF statement known as triple in RDF terminology, each consisting three parts. Subject, predicate and object, these are managed by different RDF data management like Jana, sesame, open link virtuoso, three store [2]. Simple Protocol and RDF Query Language (SPARQL) is standard query language for RDF data. Extension SPARUL is used to insert, delete and update RDF data.

RDF statement are best representing in the form of RDF graph.Fig.1 shows RDF graph representation of data. Arc labelled as a predicated and start from subject node and end at object node. Subject and object any two thing in the world, predicate is defining a relationship between subject to object.

Subject can only URI or blank node. Object can be any type, blank node, URI or literal, predicate/property only be a URI.

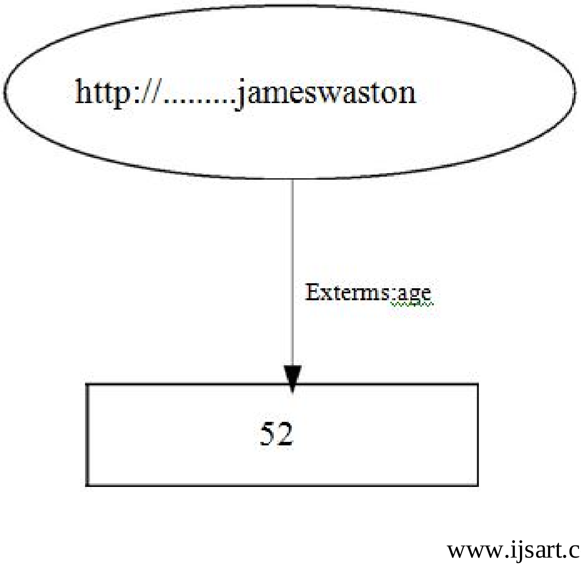
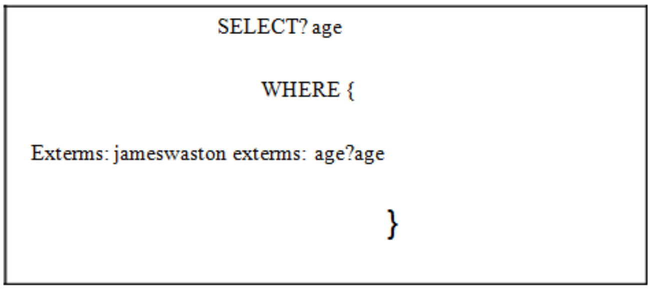


Figure1.Exmple of RDF graph

In this example jameswaston is a subject age is predicate and 52 is object value. SPARQL protocol and RDF query is semantic query language. SPARQL consist of two parts ,first part identify the variable in the query, second part graph pattern to matches against RDF graph.



```
SELECT? age
WHERE {
Exterms: jameswaston exterms: age?age
}
```

III. EXISTING SYSTEM

Only limited no. of researches concentrate database security in a semantic web. They have applied their test using Java development language .RDF data placed on jena frame work server. This system is static system, so this not sufficient security provided in semantic databases.

Limitations:

1. Java is used for the test, jena frame work server is used to place on RDF data [8].
2. It is provided only static security.
3. PHP development language is not used.
4. Sesame is not used RDF data store
5. Not provide a sufficient security.

IV. PROPOSED SYSTEM

Here proposed PHP development language is used to provide dynamicity to SPARQL queries and this provide security robustness in Semantic web and three type of authentication mechanism and hashing algorithm are used provide higher security of data's in semantic web. Fig2.shows that block diagram of proposed system.

This proposed system has been organised three main modules. 1. Request Management 2. Access control Mechanism 3. Response evaluation. Sections are described these modules and modules used algorithms techniques.

Figure.2 BLOCK DIAGRAM OF PROPOSED SYSTEM

TECHNIQUES AND ALGORITHMS:

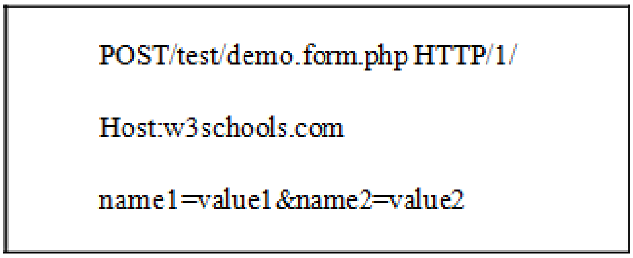
Webserver: Apache 2
Technology: PHP
Response:XML

ALGORITHMS:

MD5 hash algorithm
Access control for SPARQL request.
Parsing Algorithms (XML parser, HTML parser, SPARQL parser).

4.1 REQUEST MANAGEMENT

In this first module client send a SPARQL request message to a webserver using http POST protocol and MD5 hashing algorithms. Data transferring from client to server using POST is high secured method. Because request parameter are contained in a message body.Fig.3 shows that POST method representation.



```
POST/test/demo.form.php HTTP/1/
Host:w3schools.com
name1=value1&name2=value2
```

Figure.3.POST method

MD5 algorithm are used to produce a 128-bit hash value in the particular request. Client send to a request message to a web server, the web server decrypted particular request message and compared to client send the hash value. Two hash value are same then only webserver send a response message to a client.

4.2 ACCESS CONTROL MECHANISM

Assigning permission and access control for the system user is another suggesting solution for providing security in semantic data. In this module three type of access control mechanisms are used,

1. IP based,
2. key based,
3. Hybrid.

IP based access control mechanism server permitted client only can access data.

In a key based access control mechanism server provide particular or unique key to the particular client or companies. These key can be used to access data from the server.

Another method is Hybrid (key+Ip),key and IP are matching then only access the data. In this mechanism provide a high security.

Access control mechanism first step is configuring authentication setting, then request authentication is performed. Un authorized client is sending a request to the server, server is identified and sending a rejection message (XML without data). If authorized client is accessing data, then particular request message is accepted and then go to the request management module(module1).

4.3 RESPONSE EVALUATION

First step of this module review the request using MD5hash value, then 2 hash value are same the particular request is accepted, it is not same then rejected. If accepted the requested message Parse XML data in to PHP data structure. Then process data according to application logic.

V. CONCLUSION

Many of the researchers discussed security of semantic web in different layers. That is not provide security in databases. Limited no. of researchers concentrates data base security and some security providing mechanism is developed. But that system is static and that cannot give stuffiest security to the semantic web data. Here three type of access control mechanism and message digest algorithms are used to provide high security the database. And here using a PHP development language and to cope with new generation technologies. It Provide Dynamic security to the semantic web.

REFRENCES

[1] Fatmah Bamashmoos, lan Holyer and Theo Tryfonas and PrzemyslawWoznowski, " Towards Secure SPARQL Queries in Semantic WebApplicationsUsing PHP " in 2017InternationalConference on. IEEE, 2017.

[2] K. Sumit, and K. Suresh, "Semantic Web attacks and countermeasures." in Engineering and Technology Research (ICAETR), 2014 International Conference on. IEEE, 2014.

[3] Gabillon A. and Letouzey L., A View Based Access Control Model for SPARQL. NSS'10, 2010. pp. 105-112.

[4] O. Pablo, et. Al, "Identifying Security Issues in the Semantic Web: Injection attacks in the Semantic Query Languages." Actas de las {VI} Jornadas Científico-Técnicas en Servicios Web y {SOA}} 51: 4529-4542.

[5] X. Yang, Y. Chen, W. Zhang and S. Zhang, 'Exploring injection prevention technologies for security-aware distributed collaborative manufacturing on the Semantic Web', Int J Adv Manuf Technol, vol. 54, no. 9-12, pp. 1167-1177, 2010.

[6] A. Razzaq, K. Latif, H. Ahmad, A. Hur, Z. Anwar and P. Bloodsworth, "Semantic Security Against Web Application Attacks," Information Sciences,vol. 254, pp. 19-38, January 2014.

[7] S. Thomas, L. Williams and T. Xie, 'On automated prepared statement generation to remove SQL injection vulnerabilities', Information and SoftwareTechnology, vol. 51, no. 3, pp. 589-598, 2009.

[8] Jena.apache.org, 'Apache Jena - Parameterized SPARQL String', 2015. Available: https://jena.apache.org/documentation/query/parameterized-sparql-strings.html. [Accessed: 29- Apr- 2015].

[9] A. Medić and A. Golubović, "Making secure Semantic Web." Universal Journal of Computer Science and Engineering Technology 1, Vol. 2, pp. 99-104. 2010.