ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

Secure Agent in the Semantic Web

Rashmi Mishra[1] ,Gopal Gupta[2], Amrita Jyoti[3]

Assistant Professor, Dept. of CSE, ABES Engineering College, Ghaziabad, U.P, India [1]
Associate Professor, Dept. of CSE, ABES Engineering College, Ghaziabad, U.P, India [2]
Associate Professor, Dept. of CSE, ABES Engineering College, Ghaziabad, U.P, India [3]

Abstract—In today's world information security is most essential but there will be a need for securing information that is extracted by the agent on the web. In this paper, we will discuss security of agents on the Semantic We. Agents play different roles in different platforms dynamically changing access requirements, and users act on behalf of Use of various privileges. Agent in order to secure, we will propose a method that dynamic agent SAML authentication and authorization using them to exchange information.

Keywords— Agent, Authentication, Authorization, Semantic web, SAML (Security Assertion Markup Language)

I. INTRODUCTION

In today's worlds, data is most important and confidential on World Wide Web. Many organizations have become important sources of data, effective use of the data, exchange data and extracting information from data and use of information become important need. The data is not only integrated from the various sources but extracting information from these data pattern and tread is also important as the database. These data sources can be managed by the database management system or by data warehouse. As increasing information is going to be difficult to properly inform the way it is, to fix this problem we need to read semantic web. Semantic web concept is govern by Tim.Berners Lee, that the W3C (World Wide Web consortium) heads. Agent uses this technology to communicate with each other and carry out activities.

In order to ensure the safety of the operation, the semantic web needs privacy, trust, policies and integrity among others. To ensure the security of the operation, we need to first secure the XML and RDF layers of the semantic web. XML layer, that should be use to control over browsing, reading and revision of the different parts of the documents. There is research on XML and XML schemas to achieve. RDF has the next step. Now with the RDF not only need to secure XML, but also we need to protect the explanation and semantics.

Once XML and RDF have been secured, the next step is to check security for ontology. Ontology may have secured in some parts while some part of the ontology can be declassified security on the Semantic Web. To provide security for Semantic Web services, security models and tools for the underlying technologies, such as XML, RDF, DAML-OIL, need to be developed [8]. Especially, because intelligent agents, enabled to access and process large amounts of Web data, will be able to discover information that might be confidential, the features of interoperation and machine-enabled information processing ability may increase the danger.

II. THE SEMANTIC WEB OVERVIEW

Semantic Web, the technology proposed by a series W3C Web as the next generation, current is an extension of Web in which information is given well-defined meaning, better enabling computers and people to work in Collaboration [1]. Semantic Web more accessible to agents using means builders, such as ontology. Key component to realize Develop appropriate language for the Semantic Web and are able to encode Describing Web content.

Currently, many languages have been developed based on XML. They are RDF (Resource Description Framework), RDF Schema, DAML + OIL (DARPA Agent Markup Language? Ontology inference) layer, WOL (Web Ontology Language) and [2] so on. The facilities available in these languages to be represent concepts in a form of data processed. RDF is a foundation for processing metadata and integrating a variety of applications using XML for syntax and URIs for Naming. The difference between applications is that provides on the Web machine understandable information exchange. In addition, RDF XML description exchange uses Web resources and emphasizes facilities to enable automated Processing. DAML + OIL and OWL web ontology are Representation of knowledge based on artificial languages intelligence and intelligence and natural relationship, and describe ways to provide Classes and class instances' limits. Logical ontology of a theory to explain the meaning of Formal vocabulary and also defined a set

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

of knowledge Vocabulary, meaning interconnections, including rules and some estimates for some simple rules of logic peculiar subjects. [3] the most typical type of ontology Web classification and the conclusion is a set of rules.

In particular, A Semantic Web service ontology is a document or files that formally defines the relationship between words. Ontology can in many ways to increase Web performance. Agent-based computing helps to identify complex patterns widely distributed and heterogeneous environments [4]. To this, it is necessary to supply the data annotated comments Source so that data and information exchange with the agent considers Each other. In addition, inferring rules involved in ontology Agent helps manipulate the machine readable information enabling structured argument. The framework for agent is shown in Figure 1.

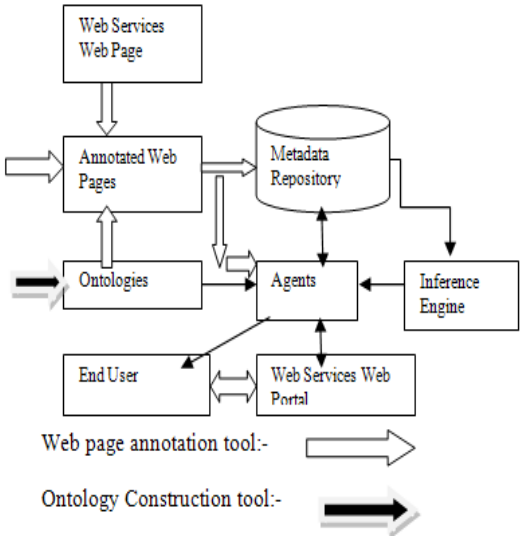

Fig. 1 The agent framework on the Semantic Web

Semantic Web as one that will reach full potential e-commerce to the electronic market place for the agent when to (semi) autonomously work [5]. Web Between heterogeneous service agent Web sites mediates, Monitors the content, inform customers, and accurate performance Filter and compare this information, in addition, Provides tailored services according to specific needs Clients, assist clients in making decisions, and acts matchmaking, server monitoring from the customer.

III. INTRODUCTION TO INTELLIGENT AGENTS

Combining descriptions from Jennings (1999) and Russell and Norvig (2003), you can understand that an agent is an encapsulated computer system made up of an architecture and a program[21]. This computer system should:

- Be positioned in some environment
- Be able to perceive its environment
- Be capable of self-governing action within that environment
- Have some kind of design objectives

An agent system is made up of four essential parts[21]:

- A performance measure
- An environment
- Actuators
- Sensors

There are four generic types of reactive agents that are traditionally discussed in texts[21]:

- Simple reflex agents, which act based on their current perceptions

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

- Model-based reflex agents, which act based on their current perceptions and partial histories
- Goal-based agents, which use their current perceptions in addition to their desires (goals) to act
- Utility-based agents, which try to maximize their status to achieve higher efficiency of acting.

IV. SAML

The OASIS Security Assertion Markup Language (SAML) specification is an industry standard for the extensible Markup Language (XML) for exchanging Authentication, attribute, and authorization information [6]. For example, such exchanges are during the interaction between applications that do not share same underlying authentication and authorization infrastructure. Organizational differences can be or based on the stage. In any case, SAML enables secure Web (SSO) to apply for single sign on between different systems and platforms. SAML statements are called assertions. They are represented as XML And construction is a nested structure, whereby An assertion can be many different Information item referring to certification, decision authority, and such properties Credentials or group membership designator. Is becoming an important standard for federal users identify and apply to both the enterprise and value chain environment that requires a user to take advantage identity that can span traditional security domains limitations.

V. SECURITY REQUIREMENT FOR AGENT

In the Semantic Web, it needs to meet the following requirements so that the agent securely works:-

(1) Agent must dynamically get security information in the real time.

(2) Agent should be able to mutually exchange security information and attribute in the heterogeneous and distributed system and platform.
(3) It is required to provide a secure channel for agent communication.
(4) It must block up attacks against the agent and the site.

VI. SEMANTIC WEB AGENT SECURITY

Trust is, usually, the important thing for people to concern when they build a system. So, why we worry about trust issue at this moment? Especially while the trust was placed on the top of the semantic web layer architecture If we agree that proof and trust are applications rather than a new ontology language on the layer stack, then it will not hurt to explore the trust issues at current stage [8][11]. There are several important results on agent trust based on psychology and security viewpoints [8][12][13][14][15]. Trust and risk are complementary terms in social relations. An emphasis on risk is generally based on mistrust, whereas trust is associated with fewer doubts about security. Those who trust others do not look for high security before they act. Trust (or security) is also one of the important issues for web service and grid computing in the semantic web pyramid [16][17].

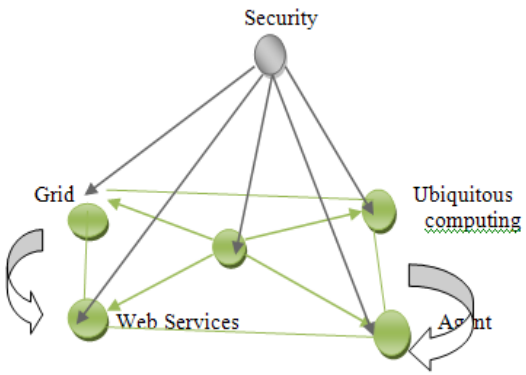

Fig.2 Basis for secure/trustful information [8] [10]

When we compare with other emerging technologies, the research progress for the trusted semantic web is very slow and the results are scarce [8][18][19].

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

VII. SECURITY SCENARIO

This scenario is the elaboration of a kind of communications between agents or the agent and platform through attribute exchange with authentication, the trusted party is responsible for asserting party and includes a component called an authentication service. It is a point of functionality for SAML processing, such as assertion generation and management. The remote site is a relying party which consumes SAML assertions and serves its resources to the agent. It contains a security service component that is point of SAML functionality and is in charge of assertion verification and management. The processing is as follows:

(1) The agent visits the site of trusted party to request a security token called assertion and sends a SAML request to the authentication service on the trusted party.
(2)The trusted party performs an access check List and requires the agent to be authenticated. Authentication is also based on the past history of the agent.
(3) If authentication is successful, the authentication services generates Security token service to an agent makes generates a SAML response. Trusted party sends a digitally signed message back to the agent.
(5) Agent accesses an application on a Agent B or on resource Site, send SAML response containing the assertion Remote site's security service
(6) The remote site's security service validates the digital signature on the SAML response. If this validates, it allows the agent to access the target resource. *An* access check is then made to establish whether the agent has the correct authorization to access the remote site and the target resource. The target resource is returned to the agent.

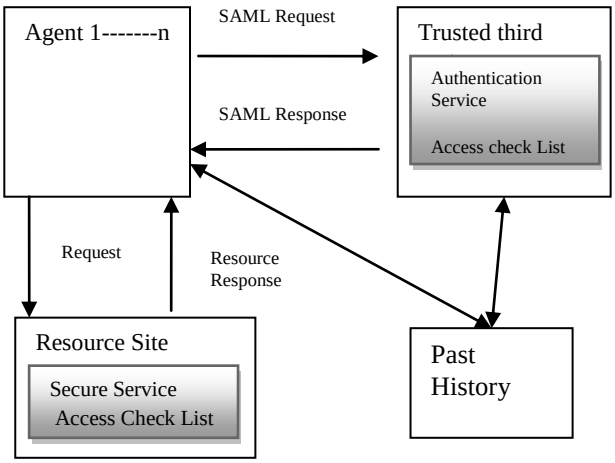

Fig.3 Security scenario shows a communication between an agent and a site using SAML

VIII. CONCLUSION

Agents were designed to support and share information. While highly desirable for the difference, it feature from the perspective of security is scary. Invalid inferences, supported Semantic Web technology by Ontologies, users may be able unauthorized use of information. In In addition to associations and meanings data with different sensitivity to repeated malicious agents can exploit statistical inferences. Although each agent can be a system a desirable and safe way to behave, their combined knowledge can be used to disclose sensitive data. Research community should therefore develop and implement technology released figures that allow control.

REFERENCES

[1] T. Bemers-Lee. et al, 2001, *The Semantic Web*, Scienfific Am.,vol. 284, no. 5, pp.3443.
[2] W3C, 2001, *Semantic Web in W3C*,http://ww\.c.\~3c.ord2UO l/sw
[3] W3C, 2001, *Web Ontology Language Overview*,httn://~vrv\v.w3. ord200 I IsdWcbOnti
[4] M.N. Nuhns, 2002, *Agent as Web Services*, IEEE Compuring, pp 93-95.
[5] B. Thuraisingham, 2002, *Building Secure survivable semantic webs*, Proceedings I4ih IEEE Internaiional Conference on Tools wirh Artificial In!elligence.
[6] *Assertion and Protocol for the OASIS Security Assertion Markup Language* (SAML) 1.0, OASIS, Nov, 2002
[7] JOO-YOUNG LEE, KI-YOUNG MOON, "*Secure Semantic Web Using SAML*", see on 21 Feb 2011.

[8] B. Thuraisingham, "*Building Secure survivable semantic webs*," Proceedings 14th IEEE
[9] CsillaFarkas,Michael N.Huhns,2002,"*Making Agent Secure on the Semantic Web*", IEEE Computing
[10] H. Yuh Jong, A Pyramid for the semantic web: Some Issues and Challenges, March 14 2003, http://www.cs.nccu.edu.tw/~jong/TPyramid/TPyramid.html
[11] D. Fensel, 2002, Layering the semantic web: Problems and Directions. In the Proceeding of 1st International semantic web Conference (ISWC, 2002). Sardinia, Italy, 9-12 June, pp: 476. ISBN: 3540437606, 9783540437604.
[12] Castelfranchi and R. Falcone, Trust and Control: A Dialectic Link. Applied Artificial Intelligence, 14 (2000), 799-823
[13] Q. He, K. Sycara and T. Finin., Personal Security Agent: KQML-Based PKI. Proceedings of the Second International Conference on Autonomous Agents, (1998).
[14] Hu, Y.-J., Some Thoughts on Agent Trust and Delegation. *The Fifth International Conference on Autonomous Agents*, Montreal, Canada, May 28 - June 1, (2001), 489-496.
[15] H. C. Wong and K. Sycara, Adding Security and Trust to Multi-Agent Systems. *Proceedings of Autonomous Agents '99 (Workshop on Deception, Fraud and Trust in Agent Societies)*, Seattle, Washington, (1999), 149-161
[16] Security in a web Services World: A Proposed Architecture and Roadmap. A joint security white paper from IBM Corp. and Microsoft Corp., Version 1.0, April 7 2002. http://www-106.ibm.com/developworks/library/ws-secmap
[17] N. Nagaratnam et al., the Security Architecture for Open Grid Services. Ver. 1, July 17 2002, http://www.globus.org/ogsa/Security/
[18] G. Jennifer, J. Hendler, and B. Parsia, Trust Networks on the semantic web. *World Wide Web Conference*, Budapest, Hungary, May 20-26 2003.
[19] Y. Gil and V. Ratnakar, Trusting Information Sources One Citizen at a Time. *The semantic web - ISWC 2002*, (2002), 162-176
[20] Adis Medić, Adis Golubović," Making secure Semantic Web", *Universal Journal of Computer Science and Engineering Technology, 1 (2), 99-104, Nov. 2010.*
[21] Lewis Daniel - in 431 Google+ circles, http://www.ibm.com/developerworks/web/library/wa-intelligentage/,21 Oct 2008