Dynamic Trust for Secure E-Shopping in Semantic Web

Kedar Nath Singh
Department of CSE
AIT, New Delhi, India

Suresh Kumar
Department of CSE
AIT, New Delhi, India

Manjeet Singh
Department of CSE
YMCA UST, Faridabad India

ABSTRACT

In the present scenario, electronic shopping has become a trend which is easy and time-saving. Such convenient services on web and the products provided by sellers are trustworthy or not are very important for buyers to know. Seller can even increase their product rating by acting as a buyer or can decrease the rating of his competitor's product. Also a buyer can also give the wrong feedback. So it is difficult to trust such e- products and user's feedback. In this paper, a dynamic trustworthy framework rectifies lack of static trust in semantic web scenario on the basis of the trust level of users (Buyers and Sellers). To achieve this, three agents are employed (namely Process Agent (PA), Detection Agent (DA) and Trust Calculation Agent (TCA)) for calculating dynamic trust in Semantic Web. These intelligent agents collectively restrict any imposter from increasing the fake trust value and hence furnish a genuine trust value dynamically.

General Terms

Dynamic, Trustworthy, Secure, Framework, Security

Keywords

Electronic Shopping, Trust, Agent, Semantic Web, Anomalous Behavior.

1. INTRODUCTION

Electronic Shopping (E-shopping) is completely a new concept to shop the desired product without going to the market. All the products and its related information can be seen and bought online (i.e. website). This service for the online shoppers is a boon as it saves time, energy, and fuel etc. This is like a virtual mall where users trust the product, seller, website and other related services on the basis of ratings and feedback.

As the technology awareness increases, popularity of e-shopping is also increasing very rapidly. The reason behind this popularity is easiness, time-saving and less hectic process. Any user can place the order online and the product gets delivered within a specified period. However, users are not more aware of the risk involved in such activities on web.

Anomalous Behavior of a user in e-shopping is defined in three categories. Firstly, when a seller acts as a buyer and gives good rating and feedback to its own product so that the buyer can trust that product. Secondly, the seller can also decrease the rating of competitor's product by acting as a buyer. This is done so that a seller can increase its product sell and market value. Thirdly, if the user is satisfied or convenience with product and other related services, even then he may purposely give wrong feedback to the provider.

The above described anomalous behavior of a user can be handled by the proposed framework in which dynamic trust of user can be calculated by the different agents in Semantic Web.

The Semantic Web is an extension of the current web in which the semantics of information and services on the web is defined. Semantic Web makes it possible for the web to understand and satisfy the requests of people and machines to use the web content [1] [2].

Figure 1 shows the basis of Semantic web, which illustrate the layered architecture of Semantic Web, where each layer takes advantage of the technologies of the previous layer. The lowest layer is the URI and UNICODE (protocol layer), and this is usually not included in the discussion of the semantic technologies.

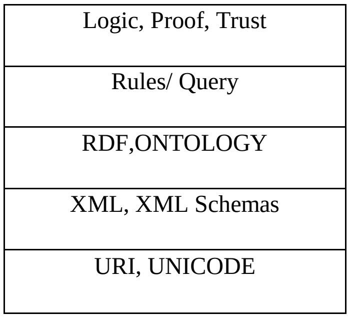

Fig 1: Basis of Semantic Web

The next layer is the XML layer. XML is a document representation language. Although XML is ideal to specify the syntax of various statements, it is difficult to specify the semantics of a statement with XML. Therefore, the W3C developed RDF. RDF uses XML syntax. The semantic Web community then went further and came up with specification of ontologies in languages such as OWL. Note that OWL addresses the inadequacies of RDF. OWL is a vocabulary extension of RDF. OWL facilitates greater machine readability of web content than does XML, RDF, and RDFS by providing additional vocabulary along with formal semantics[3].To reason about various policies, the semantic Web community has come up with Web rules language such as semantic Web rules language (SWRL) and rules markup language (RulesML) [15].

The Logic layer enables the writing of rules while the Proof layer executes the rules and evaluates together with the Trust layer mechanism for applications whether to trust the given proof or not.

As described in [4] agents on the semantic web perform task by seeking information from Web resources while communicating with other web agents. Agents are simply pieces of software that work autonomously and proactively. In most cases, agents will simply collect and organize information by utilizing metadata, ontologies, and logic.

This paper is organized as follows: Section 2 covers the literature review of the trust on user, anomalous behavior and the dynamic trust methods in e-shopping. Section 3 describes the architecture of the proposed framework and the trustworthy framework. Security Analysis of the proposed framework is given in section 4. Finally the conclusion and future work is given in section 5.

2. LITERATURE REVIEW

Number of methods has been proposed which helps in maintaining trust among users. Such method calculates the trust based on user's feedback and ratings.

Lin, Lul, Yu, Tai proposed a distributed trust framework in which trust information is managed by service brokers for users. A value of trust of all the fellows is kept by a broker and is updated after the recommendation has been checked [5]. Shmatikov and Talcott proposed a model, which defines the reputation's notion and can be used to trust reason [6].

Many trust management techniques are suggested [7][8][9][10].There are mainly two approaches for trust management in Semantic Web, Reputation Based Trust management and policy based trust management respectively [11].

There are many different ways to calculate the trust, for example Amazon takes an average of product ratings based on customer reviews. BizRate compiles the average satisfactory index about the merchant and add the product rating.

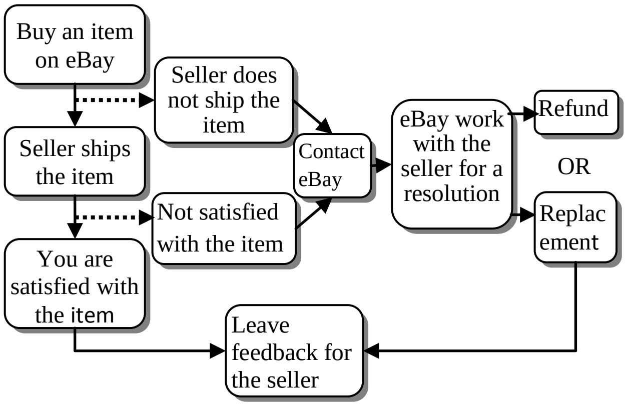
Buy an item on eBay
Seller does not ship the item
Seller ships the item
Contact eBay
eBay work with the seller for a resolution
Refund
OR
Replacement
Not satisfied with the item
You are satisfied with the item
Leave feedback for the seller

Fig 2: eBay feedback Process

eBay presents the feedback score and the percentage of positive feedbacks. Figure 2 [12] show the eBay feedback process.

The statistics which is used in calculating trust of users in e-shopping is static in nature. That is if any user is assigned with a trusted reputation then this assignment prolongs throughout. For example in eBay (eBay.com) shopping [12], the trust is calculated through feedback of the user which is static in nature. On showing any anomalous behavior, the statistics followed fails as it is not capable of calculating dynamic trust.

This framework proposed a solution to the inability of calculating dynamic trust which helps in detecting anomalous behavior of the user. This is done by using the Role Based Access Control (RBAC) [13] in which the user is assigned with a suitable role and access level based on the values of trust, threshold and reputation.

3. ARCHITECTURE OF PROPOSED FRAMEWORK

As shown in figure 3, the proposed framework comprises of four phases – (1) Authentication (2) Authorization (3) Agents and (4) Trust Calculation. A user can be a seller or a buyer. Now at first phase, he enters the login id and password if he has already registered else has to get registered. At second phase, based on the role of the user (Buyer/Seller), access rights and the authorization policies are defined. Now at third phase, an agent called process agent analyzes and controls all the activities between the user and its online shopping. Another agent called the detection agent keeps a watch on all the activities of the user and judges if any user behaves in an anomalous way. This anomalous way is defined in the first section of the paper. The last phase calculated the trust value of a user. This value is dynamic in nature and based on the behavior of user and their feedback. In this section, the four phases of the proposed framework is described in detailed.

3.1 Authentication Phase

In this phase, user enters the name (or id) and password. Then its credentials are checked in the record database and the authentication is provided. If the user is using the e-shopping for the first time then he needs to register for further processes. Once the registration is done, his credentials get saved in the record database. In subsequent authentication, his credentials match with the saved credentials.

3.2 Authorization Phase

This phase defines the role of a user and its access rights. User can be of a Buyer (B) or a Seller (S). The role of user categorization is further divided into four types which are "Most trusted user", "trusted user" "neutral user", and "un-trusted user". The type of role defined for user is based on the agent who calculates the trust of the user. This agent calculates the dynamic trust of known user based on the activities of the user.

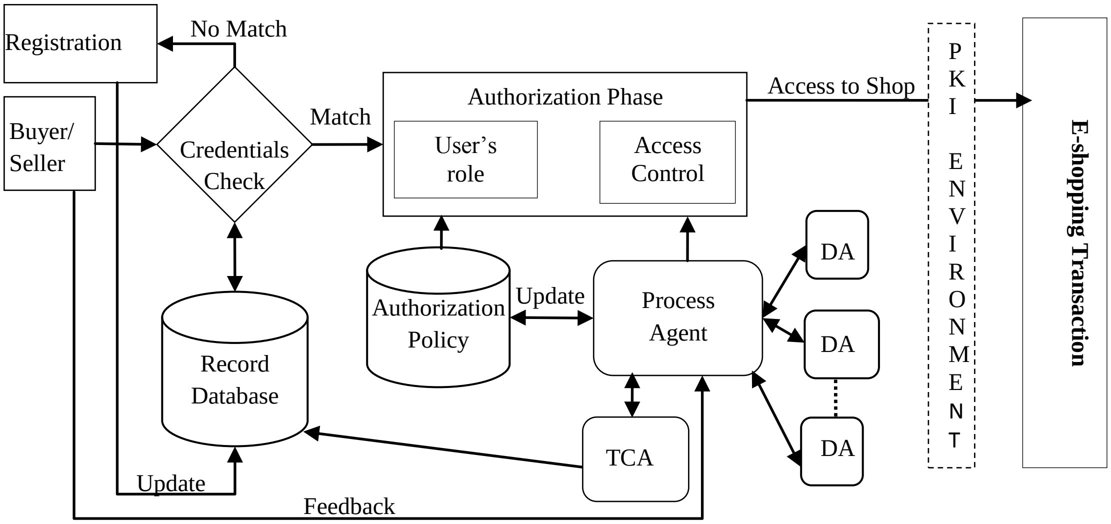

Fig3: Proposed dynamic Trust calculation Framework

As can be seen from Table 1, the Reputation and Bad activity score is defined for *Most Trusted User, Trusted User, Neutral User* and For *Un-Trusted User*. The Reputation value (U_X) and Bad Activity Score (U_Y) is defined on the scale of 5. For Example if a user is most trusted its U_X value must be 5 and its U_Y value must be less than 1.

Table 1. Reputation, BAS, Trust and Access level

Role of a User	**Reputation**	**Bad Activity Score**	**Trust level**	**Access Level**
Most Trusted User	$U_X = 5$	$0 \leq U_Y < 1$	Highest	Can buy/sell products with lowest alert credentials, certificates check and detection
Trusted User	$3 \leq U_X \leq 5$	$1 \leq U_Y \leq 3$	Normal	Can buy/sell products with low alert credentials, certificates check and detection
Neutral User	$U_X = 3$	$U_Y = 0$	Marginal	Can buy/sell products with alert credentials, certificates check and detection
Un-Trusted User	$U_X < 3$	$3 < U_Y \leq 5$	Un-Trusted	Cannot buy/sell products

Role of the user changes dynamically according to its current activity. Table 2 shows the role allotment for user according to the reputation and current Bad Activity. If a user shows anomalous behavior, the role allotted for the user is changes dynamically.

Table 2. Dynamic Change in Role

U_X \ U_Y	$U_Y = 0$	$0 \leq U_Y < 1$	$1 \leq U_Y \leq 3$	$3 < U_Y \leq 5$
$U_X = 5$	Most Trusted	Most Trusted	Trusted	Un-trusted
$3 \leq {}_X \leq 5$	Most Trusted	Trusted	Trusted	Trusted
$U_X = 3$	Neutral	Neutral	Trusted	Un-Trusted
$U_X < 3$	Un-Trusted	Trusted	Un-Trusted	Un-Trusted

For example a role allotment for new user is as follows: if a user is new user, and he request for buy a product, then this new user is allotted a role as *Neutral user*. Role is dynamically changes. It can be changed based on the current activities (Bad Activity score). Most of the E-shopping centers (virtual malls) are statically allots the role, but static allotment is not more convenient. In this model role is allotted dynamically which is more appropriate. For Example user role can be change from *Neutral user* to *Trusted user* as follow: If the current bad activity is less than 3 and overall reputation is more than 3, or a role of an user can changes from *Trusted* to *Un-Trusted* if reputation U_X become less than 3 and bad activity score U_Y become more than 3. In this way role of the user is changes and hence access control.

3.3 Agent Phase

PA (Process Agent) is the main agent, which coordinates all the agents involve in the framework. PA is responsible for role allotment and access control of a user. PA updates the authorization policy dynamically. For example if a user traced as un-trusted PA changes its authorization policy spontaneously and restrict from shopping. Moreover, PA handles and communicates with DA (Detection Agent) in order to get update about user's activity. PA also communicates with TCA for dynamic trust calculation.

Detection agent (DA) is responsible for detecting any anomalous activity of a user. Anomalous activities like if any seller logins as a buyer to increase the rating of its own product or to decrease the rating of other's product in order to increase its business etc. On detecting such activity, DA informs the process agent and then PA enquires the Trust Calculation Agent (TCA).

3.4 Trust Calculation Phase

Trust calculation of a user is performed by an agent called Trust Calculation Agent (TCA).The trust calculated for a user is dynamic in nature and can be changed. TCA calculated the trust based on the information stored in the record database (Reputation), feedback from the user and the current activities of a user. This current activity is measured with the help of DA. DA informs PA about user activities and then PA sends an update to TCA to calculate the trust value of that user. This is simply average of above three parameters feedback, previous Reputation value and current Bad Activity Score. This value is updated dynamically in each transaction and saves into record database.

All the users have a reputation which is based on the previous activities performed by them. These activities are stored in the record database. The Reputation value will varies from 0 to 5. This reputation of a user is calculated by TCA and maintained in the record database.

Trust value of a user can increment and decrement based on the current activities and feedback. If a user has good behavior in the record database and then suddenly he starts showing anomalous behavior then this gets detected by the DA and then informs PA. Further PA sends the current status of that user and then TGA calculates the trust value again and degrades its trust value. This user again can increment its trust value by showing good behavior.

Based on the new trust value of that user, it is updated in the authorization policies where user's role, its access rights, reputation and trust levels are defined.

PKI (Public Key Infrastructure) in Semantic Web [16] environment provides the digital certificates to the user for buying products. The entire authenticated and authorized user has this certificate which proves their legitimacy. If any user does not provide the certificate then that user will automatically get isolated from the shopping transactions.

4. SECURITY ANALYSIS OF THE FRAMEWORK

The security analysis of the proposed framework is described in this section. This section deals with how all the security principles like confidentiality, integrity, availability, authentication and non-repudiation are maintained in the proposed framework which are as follows.

4.1 Confidentiality

All the data related to sellers and buyers are individually isolated from each other. For example a seller cannot even come to know about the financial status of the buyer. Even the trust values of the users maintain by the agent are not accessible either by seller or buyer.

4.2 Integrity

All the transaction taking place through this framework cannot be modified by any intruder or by any user. Even the user information is secured in the Record database cannot be manipulated.

4.3 Availability

A 24/7 services are available to the user. They can buy or sell the product at midnight also, such availability of service on the web save the valuable time of the user.

4.4 Authentication

Authentication in the proposed framework provides access to the legitimate user for shopping.

4.5 Non-repudiation

In PKI environment [16], digital signature are used which helps in providing the Non-repudiation on service. In other words, any user cannot deny from any transaction being processed from his side.

5. CONCLUSION AND FUTURE WORK

In this paper, a framework is proposed which provided dynamic trust value of a user with the help of three agents called process agent, detection agent and trust calculation agent. The dynamic trust of a user means that user can be a trusted user at one time but on showing any anomalous behavior it can become a null or an un-trusted user. This calculation of dynamic trust is based on the record database information, current activity and the feedback from the user. Therefore, proposed framework is useful in calculating dynamic trust and resists any anomalous behavior of a user.

The proposed framework can be deployed using JADE (Java Agent Development framework) [14] where agents are designed with an in-built intelligence. JADE is fully compliant with FIFA-ACL specification. Agent can effectively communicate with each other using FIFA-ACL based communication protocol. Thereby, the effectiveness of this proposed framework can be determined and how can it can detect and restrict any user on showing any anomalous behavior.

6. ACKNOWLEDGMENT

I, Kedar Nath Singh would like to thank my college, Ambedkar Institute of Technology (situated at New Delhi) for providing me adequate resources to make this paper. I would like to thank my guide Mr. Suresh Kumar for his valuable suggestions. Also I would like to thank Dr. Manjeet Singh for his valuable comments.

7. REFERENCES

[1]. Berners-Lee, T.B, and J. Hendler, "The Semantic Web," Scientific American Magazine, 17 May 2001

[2]. W3C Semantic Web Frequently Asked Questions". W3C. www.w3.org/2001/sw/SW-FAQ.

[3]. W3C, OWL web Ontology language overview, http://www.w3.org/TR/2003/WD-owl-features-20030331/.

[4]. Berners-Lee, Godel, and Turing, "*Thinking on the Web*," Second Edition, JOHN WILEY & SONS, 2009, pp xxvi.

[5]. Kwei-Jay Lin, Haiyin Lu1, Tao Yu, and Chia-en Tai. "A Reputation and Trust Management Broker Framework for Web Applications," 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'05).

[6]. V. Shmatikov and C. Talcott, "Reputation-Based Trust Management." Journal of computer security, vol.13, No. 1, 2005, pp.167-190.

[7]. Katebi, M., Katebi S.D, Trust Models Analysis for the Semantic Web. IEEE 2009 Second International Conference on Developments in e-Systems Engineering (DESE).

[8]. A. Josang, R. Ismail, and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," *Decision Support Sys.vol 43*- no. 2, 2005, pp. 618–44.

[9]. Jennifer Golbeck, James Hendler. Inferring reputation on semantic web. *WWW 2004*, May 17-22, 2004, New York, NY USA. ACM.

[10]. Matthew Richardson, Rakesh Agrawal and Pedro Domingos, "Trust Management for Semantic Web," the second international Semantic Web conference, Senibel, Island, 2003, pp 351-368.

[11]. P.A. Bonatti, C. Duma, D. Olmedilla, "An Integration of Reputation-Based and Policy-Based Trust management in proceeding of the Semantic Web policy workshop, Galway, Ireland, nov.2005.

[12]. http://pages.ebay.in/aboutebay/eBay_Guarantee.html, access on May -4- 2011.

[13]. Feinstein, R. Sandhu, E. Coyne, and C. Youman, "Roll-Based Access Control Model," IEEE Computer, 29(2), 1996, pp. 38-47.

[14]. F. Bellifemine, G. Claire, D. Greenwood, "*Developing Multi-Agent Systems with JADE*," John Wiley & Sons.2007.

[15]. Bhavani Thuraisingham, "Building Trustworthy Semantic Web," Auebach Publication 2008, pp.72-73.

[16]. S Kumar, R.K. Prajapati, M. Singh, A. De, "Security Enforcement Using PKI in Semantic Web," Computer information systems and industrial management applications (CISIM) 2010, IEEE.