Available online at www.scholarsresearchlibrary.com

Scholars Research Library

European Journal of Applied Engineering and Scientific Research, 2012, 1 (2):61-65

(http://scholarsresearchlibrary.com/archive.html)

ISSN: 2278 – 0041

Privacy preserving reputation system for virtual marketplaces

Nungleppam Gopil Singh[*], Loitongbam Basantakumar Singh

Department of Computer Science and Engineering, Tezpur University, Tezpur, Assam, India.

ABSTRACT

With the advent of virtual marketplaces or so called online shopping sites, trust and reputation system plays a significant role in the decision making between buyer and seller or two parties. The basic idea to trust other is mostly through its reputation which is natural and is already successfully used for online commercial applications. Reputation is generally computed from the accumulative ratings that are given when two or more transacting parties transact. But preserving privacy among transacting parties and among others has become a mandatory and necessity due to problems from defamation, monopoly, and enmity among sellers which give rise to compromise in the reputations. The main application area of this work is in the virtual marketplaces but, can also be used for online communities, social network and various other services where reputation systems may be used. The main advantage of this method is to give a better, accurate and more robust reputation system which is having resistance from manipulation. The main challenge is the extra overhead of the reputation engine which if fails collapses the whole system. So to avoid this, a better or stable server may be used as a server for reputation engine. The main aim of this work is to provide privacy among parties so that a robust and better as well as accurate reputation may arise. Thus we proposed a model for privacy preserving reputation system for virtual marketplaces using web based technology. Here in this work pseudonym and cryptographic techniques are used to achieve this.

Keywords: trust, reputation, pseudonym, cryptographic, web based

INTRODUCTION

Reputation systems play an important role in the decision making between two parties in order to trust one another. As it is natural for human beings to trust people which has high reputation. A reputation system computes the reputation score, which is the basis of trust, from the feedback ratings given by other parties for that party. The reputation score helps in deciding to trust or not to trust by other party. Reputation systems are successfully implemented in commercial online applications *viz.*, e-commerce. For example eBay and Amazon uses their reputation systems to discourage fraudulent parties. The EigenTrust[3] reputation system is used to filter inauthentic content in peer to peer file sharing.

A reputation score is a function of the feedback values provided by other parties. Thus reputation system is accurate if and only if feedback is accurate. However this is theoretical but in practical people tends to give false feedback [2]. The reasons for false feedback may include fear of retaliation, mutual understanding between parties, defamation, enmity and sometimes pessimist persons. For example, originally eBay allows buyers and sellers to rate each other a positive, neutral or negative feedback but to counter the retaliatory effects from sellers, it now prohibits sellers from leaving a neutral or negative feedback. But this solves just one case and does not counter from defamation by a group of buyers.

A general solution to the above problem is to compute reputation systems while preserving privacy such that the burden of retaliatory effects of parties are removed and instruct to give an honest feedback. In this article we focus on privacy preserving reputation systems for centralized environments. The most common example of centralized environment is the virtual marketplaces also known as online shopping websites. However the basic privacy preserving reputation systems on online shopping websites suffer from defamation and dishonest buyers.

2 PRIVACY PRESERVING REPUTATION SYSTEM

2.1 PRECONDITIONS

Privacy preserving means that the identities of the transacting parties must be hidden from one another as well as the ratings they give as feedback must also be hidden amongst them.

In this article we present a system that preserve privacy and counter the following cases, among others, which may arises if privacy is not properly preserved.

Case1:
Buyer A fears the consequence of retaliatory effects of negative and neutral feedback. So buyer A gives a false or inaccurate feedback to seller B.

Case 2:
Buyer A and seller B know each other and have a mutual understanding to increase their reputation score and gives false feedback of high rating to each other.

Case 3:
Buyer A knows seller B and is an agent or friend of seller C which is in competition with seller B so a false feedback is given (in the behalf of seller C - collusion) so that the reputation score of seller B decreases.

Case 4:
Buyer A is a pessimist and thinks that if seller B is given a negative feedback it will improve the service more on next time so a false feedback is given.

Case 5:
Seller usually knows the shipment address of the buyer and sometimes phone number, so unnecessary advertisements of products may occur. This is considered to be a hindrance to personal life of the buyer.

If privacy is not preserved properly the above cases may arise leading to a false reputation score or uneasiness in personal life. So to counter these, following solutions had implemented before.

2.2 PRESENT SCENARIO:

To better understand how privacy can be preserved in reputation systems, from amongst the reviewed work, four of the most related work are presented and discussed in the following section.

2.2.1 Solution by eBay:

No negative or neutral feedback can be given by seller. Thus case 1 is solved but this solution fails to counter the remaining cases.

2.2.2 Solution by Gudes, E., *et al.*

According to Gudes, E., *et al*. [6] they address the following problem: A needs to compute her trust in the expert, based on the experience other members of the community have had with this expert. They use the Trust-set as the group of members participating in this computation. The trust of A in x using Trust-sets [5] can be computed according to:

$$TE(A,x) = \frac{\sum_{B_i \in TrustSet(A), DTE(B_i,x)\neq\perp} DTE(B_i,x)\cdot TM(A,B_i)}{\sum_{B_i \in TrustSet(A), DTE(B_i,x)\neq\perp} TM(A,B_i)}$$

where:
$DTE(B_i,x)$ is the trust member B_i has in expert x based based on its own accumulated experience.
$ITE(A,B_i,x) = TM(A,B_i)\cdot DTE(B_i,x)$ is the indirect trust member A has in expert x based on B_i direct trust in x

With an assumption that $TM(A,B)$ is known to agent A since it reflects its private information. Thus the denominator is easy to compute by A without disclosing private information. The nominator is a sum of products of two terms, the first one is assumed to be distributed among the agents B_i and is known only by its corresponding agent, and the second one is known to A. Therefore the challenge they face is to privately compute the following sum of products denoted by

$$\rho(A,x) = \sum_{\forall B_i \in S} DTE(B_i,x) \cdot TM(A,B_i) = \sum_{\forall B_i \in S} DTE(A,B_i,x)$$

Where S denotes the trust set of A.

2.2.3 Solution by Schiffner, S., *et al.*[1]:

A pseudonym is used between two parties for the communication and ratings. But ratings itself is visible. And case 5 occurs and is vulnerable to case 1.

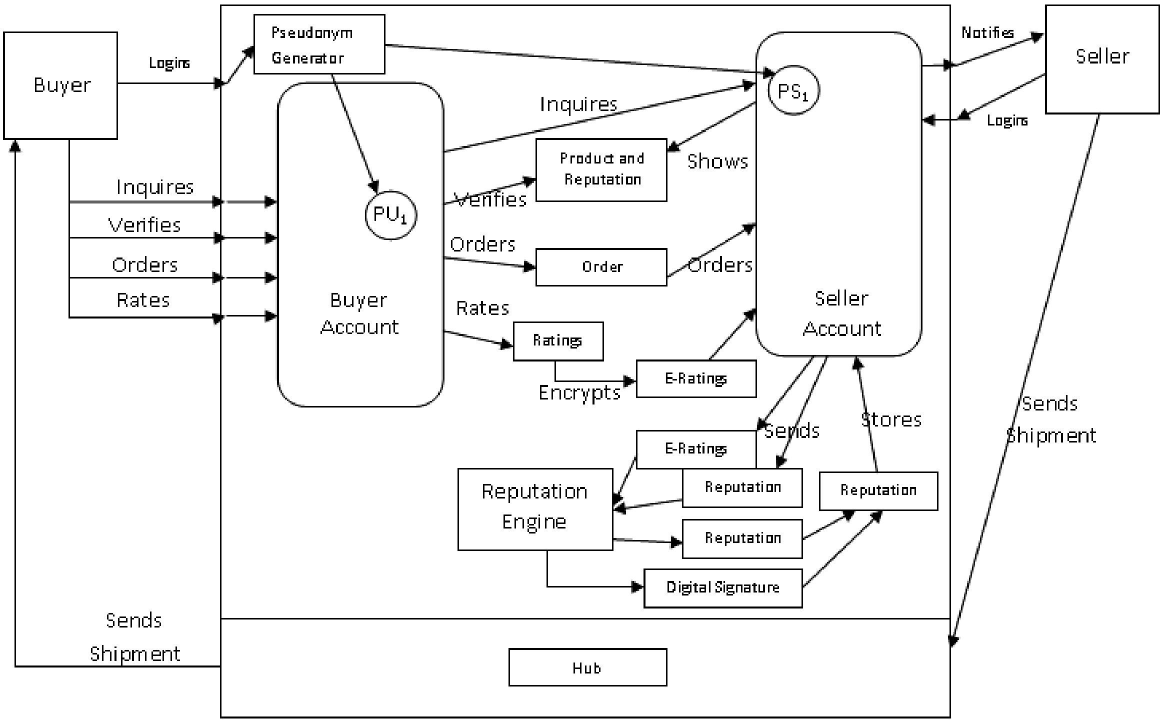

Figure 1: Overview of privacy preserving reputation system.

2.2.4 Solution by PGP trust model :

Pretty Good Privacy [8], or commonly known as PGP is a milestone in the history of cryptography, for its first time introduction to the privacy required on-line public. PGP was originally created for encrypting e-mail messages using public or conventional key cryptography. While the conventional cryptography techniques are used mainly to encrypt local files. PGP first generates a random session key with which the plain-text is encrypted; later this session key along with the cipher-text is encrypted using the public key of the recipient and later forward to the recipient. Other features include generation of message digest, generating digital signatures, management of personal 'key rings' and distributable public key certificates. It is also designed to work in off-line scenario to facilitate e-mail and file encryption rather than on-line transactions.

In PGP trust architecture it follows 'web of trust' [7] where there is no specific central authority which everybody trust. Rather it creates a web of individual’s public key interconnected by links formed by signing each other's public key.

2.2.5 A General Solution:

A general solution to the above cases is by the implementation of privacy preserving Reputation System. Thus to solve the above scenario we present a system which can counter all the mentioned cases by preserving a proper privacy.

2.3 SYSTEM OVERVIEW

For our system, we assume an online store where users register as seller or buyer and rate each other depending upon their performance and response. Let S be the seller account and U be the buyer account. When U wants to buy something from the online store it searches the store. The store returns the search with product along with the seller's reputation score. The buyer then decides from whom the product should buy by seeing the price and reputation score from the list returned from the search.

After decision the selected product is added to the order list and orders the product. The buyer selects appropriate payment method and pays the order. The seller then receives the order and processes it and later ships the order to the buyer. The buyer then receives the order and according to the response of the seller it gives a feedback score and rates the buyer, similarly the seller also gives a feedback of the buyer. The reputation engine computes the reputation from these feedback ratings and the reputation score is stored to each user. Figure 1 shows the actions performed by the users and the system among registered users.

2.3 SYSTEM DETAILS

In this section we describe about the workings and structure of the system. Users who want to use the system should register on the system to get a reputation account. Both buyer and seller who register are given an initial reputation score. The seller adds the products which are going to be sold by him in his registered account. A buyer who wants to buy a product logs in the system. At the time of login the buyer is assigned a pseudonym PU1 through which all the communications will be done. The pseudonym creates anonymity of the user.

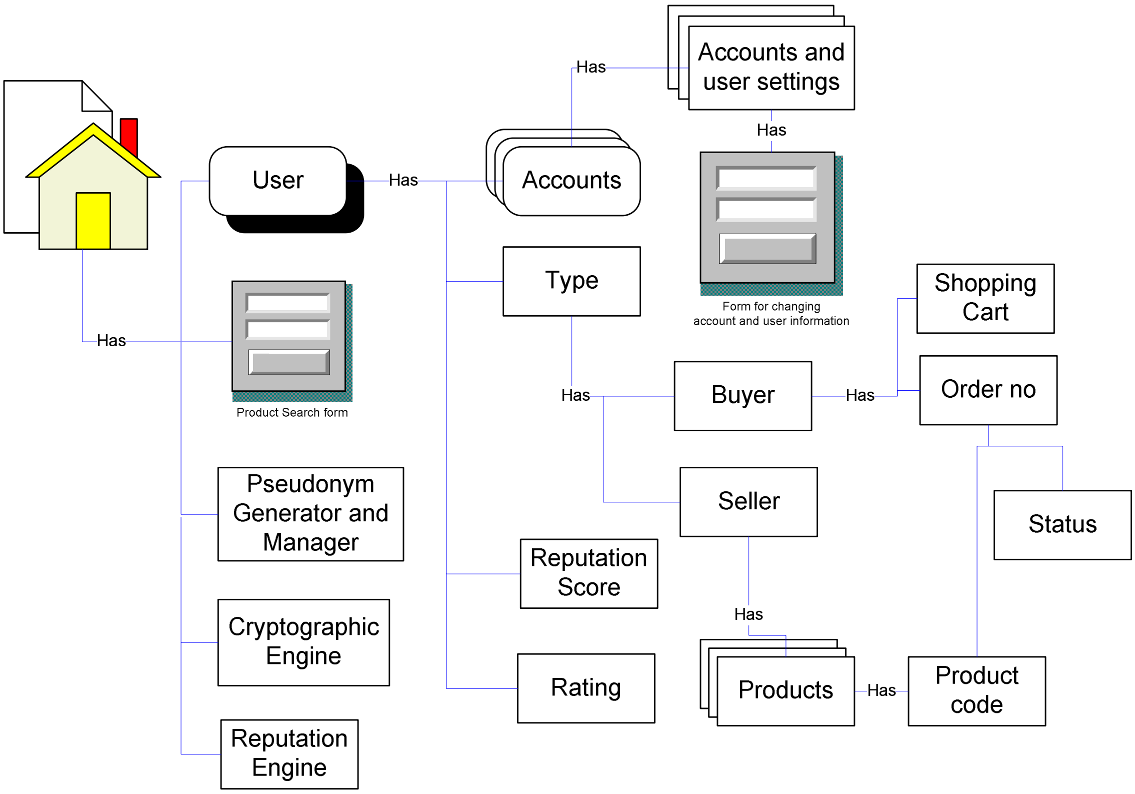

Figure 2: Website organization of the privacy preserving reputation system.

The buyer searches the system for a product. The system then returns the buyer with the products offered by the sellers and its availability along with a pseudonym assigned for each seller. The buyer views the product description price and reputation score and decides which product to choose from which seller.

The buyer then orders the product. The system assigns the order with an order code and the buyer selects an appropriate payment method and pays for the order. The seller is then informed about the order by the system. The payment is taken in custody to the system till the product is shipped by the seller.

The seller then ships the order to the system as the identity of the buyer is unknown to the seller and informs about the shipment to the system. The system after receiving the order validates the order and ships to the buyer as only the system knows the whereabouts of the buyer. The system then releases the halted payment to the seller. The buyer upon receiving of the order login in the system and sets its order received status and gives a feedback about the seller. The feedback is encrypted using a public key encryption with public key of the system and stores it to the seller account. The feedback is not visible to the seller. The seller also gives a feedback to the buyer and is similarly processed and stored. The reputation engine then computes the reputation of each user from time to time by using the feedback ratings stored against each user and the previous reputation score of the user. Only the reputation engine can view the feedback ratings as the private key is posses by the reputation engine. The computed reputation score is then digitally signed by the engine and stored to respective user accounts.

The system Model can be implemented in a website with user-roles and dividing various modules for interaction to user i.e. buyer and seller an overview of this website model is shown in figure 2. The website consist of, pseudonym generator and manager module, cryptographic engine, and Reputation Engine, along with the user and its related information. Only the user logged in can view and edit its own personal information. This makes it a hard privacy preserving system. Only the administrator at the hub knows the user information for processing of shipments.

CONCLUSION

We presented an easy yet effective privacy preserving reputation system for computing reputation in an online shopping website. Privacy is preserved in the system using anonymity and public key encryption. Security and guarantee of the money back is achieved using payment protocol by taking payment in stake. Thus the risk of losing money in also reduced. Above all the reputation engine used for the system is not so critical; any engine should give better results as the ratings given will be more accurate for normal users. The cryptographic techniques used will make the system more robust as the ratings is not directly visible to anyone, except the reputation engine. The use of a central hub can be a problem if the members of the hub become a seller or disclose the privacy of users. This can be avoided by signing non disclosure agreement. Other than the above case the privacy of the user are preserved not only while computing reputation scores but also all the time. The one point failure of the system is the web hosting where the main web application should be hosted which may suffer if the server fails. These are a condition for all online applications and are countered using parallel servers and other methods. The main disadvantage of this system is the shipment cost is increased. The system may also be adapted to other systems like, peer to peer networks, online communities, and where reputation systems can be used with minor changes and adaptations.

REFERENCES

[1] S. Schiffner, S. Clauß and S. Steinbrecher, In: T. Gyimóthy(Ed.), I. Černá(Ed.), J. Hromkovič(Ed.), K. Jeffery(Ed.) and R. Královič(Ed.), International conference on current trends in theory and practice of computer science, 22-28 Jan. 2011, Nový Smokovec, Slovakia (Springer-Verlag Berlin, Heidelberg, **2011**) 506-519.
[2] P. Resnik and R. Zeckhauser, Advances in Applied Microeconomics, Emerald Group Publishing Limited, Bradford, **2002** ,11, 127-157.
[3] S. D. Kamvar, M. T. Schlosser & H. GarciaMolina, In: Yih-Farn Robin Chen(Ed.), László Kovács(Ed.), Steve Lawrence(Ed.), International conference on World Wide Web,20-24 May. 2003, Budapest, Hungary(ACM New York, USA **2003**) 640-641.
[4] S. Schiffner, S. Clauß and S. Steinbrecher, In: Fabio Martinelli(Ed.), Bart Preneel(Ed.), European conference on Public key infrastructures, 9-11 Sept. **2009**, Pisa, Italy (Springer-Verlag Berlin, Heidelberg, **2010**) 209-224.
[5] D.W. Manchala, International Conference on Distributed Computing Systems, 26 - 29 May. 1998, Amsterdam, Netherlands (IEEE Computer Society Washington DC, USA, **1998**) 312-321.
[6] E. Gudes, N. Gal-Oz and A. Grubshtein, In: E. Gudes(Ed.), J. Vaidya(Ed.) , Working Conference on Data and Applications Security XXIII, 12-15, July. **2009**, Montreal, Canada (Springer-Verlag, Berlin, Heidelberg, **2009**) 291 – 298.
[7] W. Stallings, *Byte*, **1995**, 20, 2, 161–162.
[8] P. R. Zimmermann, An Introduction to Cryptography, Network Associates Inc. , USA, **2004** available as https://download.pgp.com/pdfs/Intro_to_Crypto_040600_F.pdf, accessed on 25th September **2011**.