ISSN: 2321-7782 (Online)
Volume 3, Issue 1, January 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

A Review on Privacy Preserving Reputation Protocol for Disruptive Malicious Models

Neena B S[1]
PG Scholar, Department of Computer Science
College of Engineering Perumon
Kerala, India

Remya R[2]
Assistant Professor, Department of Information Technology
College of Engineering Perumon
Kerala, India

Abstract: ***The privacy preserving reputation protocol provides the users with honest feedback while preserving their privacy in an online auction or e-commerce site. It helps the users to ensure that the rating they provide is not affected by any malicious agents and it will not cause any negative impact in the future. This paper gives a brief description on different privacy preserving reputation protocol [2] in decentralized reputation system [5]. Each protocol is used to compute reputation of a user and each protocol may vary in their strength in terms of preserving privacy. If the protocol is efficient then the users can provide accurate feedback and can compute accurate reputation of a user. It will be a great benefit for the users in virtual communities.***

Keywords: Reputation protocol, malicious agents, decentralized reputation system, k-share, zero knowledge.

I. INTRODUCTION

A virtual community [7] is a community of strangers where users don't reveal their identities. In a reputation system users communicate irrespective of their trustworthiness and will use others reputation score to decide whether to communicate or not. A reputation score is computed based on the feedback provided by the user. A high reputation score means a reputed user.

A centralized reputation system has a centralized reputation database where all the data are securely stored. But in a decentralized reputation system there is no such central repository and each participant is responsible for his own data. Hence there is a greater chance of attack by malicious agents. If a malicious agent learns the private feedback value of a reputed user he can misuse the value and it will create a negative impact for the reputed user.

The privacy preserving reputation protocol helps the users to provide their honest feedback irrespective of any attacks from malicious agents. As a result the reputation system works well under any malicious attack. By using this protocol, reputation score of users can be computed in a privacy preserving manner. A privacy preserving protocol can be either cryptographic or non-cryptographic.

II. ADVERSARIAL MODELS

a. Semi honest agents:

Semi honest agent strictly follows the protocol for computing the reputation score of a user and is curious about the private feedback value of other users. They use the intermediate information exchanged in between the execution of the protocol to get the private feedback value of other users.

b. Non disruptive malicious agents:

They are not bound to the protocol and they may deviate from the protocol when necessary. They may use extra protocol activities to learn the private feedback of other users. They do not intend to disrupt the protocol but has the intention-to learn the private feedback of other users.

c. Disruptive malicious agents:

These agents have the same goal as that of non-disruptive malicious agents. The difference is that disruptive malicious agents not only learns private feedback of other agents but also have other intentions.

This paper describes different privacy preserving reputation protocol that is against above adversaries.

III. Different Privacy Preserving Reputation Protocols

a. Secure Sum

This protocol [6] is used to compute the reputation value of multiple sites and keeping the data private. It can be a secure multi-party computation. This protocol is related to zero knowledge proof in which one party can prove to another party that the given statement is true without revealing other information.

b. *Protocol against semi honest adversaries.*

In this protocol the agents itself will select their trustworthy agents to share the intermediate information. The main two advantage of this protocol is that since agents itself select the trustworthy agents the probability of preserving privacy is maximum and also each agent exchanges message with a constant number of other agents. Hence communication complexity is linear.

c. *Protocol against non-disruptive malicious adversaries*

There are two ways in which the local feedback values of an agent can be leaked. First, by the exchange of intermediate values during the execution of the protocol and the attacker will use this intermediate values to find the local feedback value.

Second, an attacker observes the reputation of an agent before and after the agent updates its local feedback. Since the reputation is computed in an additive manner [4] an attacker can find the private local value as a difference between previous and current local feedback. This protocol is against these two attacks.

d. *Protocol against disruptive malicious adversaries.*

This protocol is against strong malicious attacks. It is a cryptographic protocol while other mentioned protocols are non-cryptographic. The cryptographic system used in this protocol is paillier cryptosystem [3]. This protocol is also known as Malicious k-share protocol [1]. An agent can preserve its privacy by partially trusting only k feedback providers. Hence it reduces the complexity of trusting the whole users in the environment. It allows the users to check their privacy before sending their feedback. It prevents the malicious agents from making erroneous computation.

IV. Advantage

The main advantages of these privacy preserving reputation protocol is

- Can be effectively used in decentralized environment
- Less computation complexity
- Provide greater privacy for the users.
- No need of any trusted third party.

V. CONCLUSION

This paper gives a brief description on different privacy preserving reputation protocols that are against different adversarial models. This paper also describes different types of adversaries such as semi honest agents, non disruptive malicious agents and disruptive malicious agents. Among the protocols described the most effective and efficient protocol is malicious k-share protocol since it is a cryptographic protocol. These protocols mainly encounters two types of attacks-attacker gaining information from intermediate values and attacker gaining information from the updating agent's local feedback. These protocols provide users the advantage of providing honest feedback by preserving their privacy which helps in the accurate computation of reputation score.

ACKNOWLEDGEMENT

Our sincere thanks go to all the teaching and non-teaching staffs in Department of Computer Science and Engineering for their help and cooperation throughout the work.

References

1. Omar Hasan, Lionel Brunie, Elisa Bertino, and Ning Shang," A Decentralized Privacy Preserving Reputation Protocol for the Malicious Adversarial Model", IEEE transactions on knowledge and data engineering year 2013.
2. E. Gudes, N. Gal-Oz, and A. Grubshtein, "Methods for computing trust and reputation while preserving privacy," in Proc. of DBSec'09, 2009.
3. P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proceedings of the 17th International Conference on Theory and Application of Cryptographic Techniques, 1999.
4. E. Pavlov, J. S. Rosenschein, and Z. Topol, "Supporting privacy in decentralized additive reputation systems," in Proceedings of the Second International Conference on Trust Management (iTrust 2004), Oxford,UK, 2004.
5. O. Hasan, L. Brunie, and E. Bertino, "Preserving privacy of feedback providers in decentralized reputation systems," Computers & Security, vol. 31, no. 7, pp. 816 – 826, October 2012,http://dx.doi.org/10.1016/j.cose.2011.12.003.
6. http://en.wikipedia.org/wiki/Secure_multi-party_computation
7. P. Resnick and R. Zeckhauser, "Trust among strangers in internet transactions: Empirical analysis of ebay's reputation system," Volume 11 of Advances in Applied Microeconomics, pp. 127–157, 2002.

