Future Generation Computer Systems 62 (2016) 175–189

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Two Schemes of Privacy-Preserving Trust Evaluation

Zheng Yan [a,b,*], Wenxiu Ding [c], Valtteri Niemi [c,d], Athanasios V. Vasilakos [e,f]

[a] State Key Laboratory of Integrated Services Networks, School of Cyber Engineering, Xidian University, China
[b] Department of Communications and Networking, Aalto University, Espoo, Finland
[c] State Key Laboratory of Integrated Services Networks, Xidian University, China
[d] Department of Computer Science, University of Helsinki, Finland
[e] University of Western Macedonia, Kozani, Greece
[f] Lulea University of Technology, Sweden

HIGHLIGHTS

- Two security schemes for Privacy-Preserving Trust Evaluation (PPTE).
- Trust evaluation algorithms cooperating with the PPTE schemes to resist internal attacks.
- Security and performance proof of two PPTE schemes through analysis and implementation.
- Feasibility to support various scenarios with either small or big evidence data.

ARTICLE INFO

Article history:
Received 27 May 2015
Received in revised form
21 October 2015
Accepted 4 November 2015
Available online 1 December 2015

Keywords:
Trust evaluation
Homomorphic encryption
Privacy preservation
Secure multiparty computation
Big data

ABSTRACT

Trust evaluation computes trust values by collecting and processing trust evidence. It plays an important role in trust management that automatically ensures trust relationships among system entities and enhances system security. But trust evidence collection and process may cause privacy leakage, which makes involved entities reluctant to provide personal evidence that is essential for trust evaluation. Current literature pays little attention to Privacy-Preserving Trust Evaluation (PPTE). Existing work still has many limitations, especially on generality, efficiency and reliability. In this paper, we propose two practical schemes to guard privacy of trust evidence providers based on additive homomorphic encryption in order to support a traditional class of trust evaluation that contains evidence summation. The first scheme achieves better computational efficiency, while the second one provides greater security at the expense of a higher computational cost. Accordingly, two trust evaluation algorithms are further proposed to flexibly support different application cases. Specifically, these algorithms can overcome attacks raised by internal malicious evidence providers to some extent even though the trust evaluation is partially performed in an encrypted form. Extensive analysis and performance evaluation show the security and effectivity of our schemes for potential application prospect and their efficiency to support big data process.

1. Introduction

Trust evaluation plays an important role in trust management. It is a technical approach of representing trust for digital processing, in which the factors influencing trust are evaluated based on evidence data to get a continuous or discrete number, referred to as a trust value. In the literature, several theories, including Bayesian inference, weighted average models, subjective logic, Dempster–Shafer theory, fuzzy logic and entropy-based models, are applied to model and evaluate trust and reputation (i.e., public trust) [1]. All of above methods generate trust values by analyzing and computing evidence data collected from a number of evidence providers. Many existing methods contain evidence summation in the process of trust evaluation. Nowadays, trust evaluation has been widely applied in various fields of computer, communication and information systems. It assists in automatically ensuring trust relationships among system entities and enhancing system security.

* Corresponding author at: State Key Laboratory of Integrated Services Networks, School of Cyber Engineering, Xidian University, China.
E-mail addresses: zyan@xidian.edu.cn, zheng.yan@aalto.fi (Z. Yan), wenxiuding_1989@126.com (W. Ding), valtteri.niemi@cs.helsinki.fi (V. Niemi), th.vasilakos@gmail.com (A.V. Vasilakos).

http://dx.doi.org/10.1016/j.future.2015.11.006
0167-739X/

1.1. Motivation

Trust is normally evaluated based on the evidence that shows a trustor's belief on a trustee. Typical examples of evidence include feedback on the performance and quality of the trustee, observed performance or behavior of the trustee, and recommendations on the trustee. In many scenarios, a trustor entity conducts trust evaluation according to personal experiences and the evidence collected from other entities. For example, a reputation server collects individual feedback or votes from many users about a trustee entity (e.g., a mobile application, a movie, a service, or a networking node) for reputation generation. In social networking, social trust can be assessed based on social interaction experiences and feedback collected from a sufficient number of credible individuals.

However, trust evaluation could impact the privacy of involved entities. Obviously, processing and analyzing collected evidence data could reveal sensitive information of providers such as personal preferences, opinions and interests. The evaluation may also intrude the privacy of the entity being evaluated. Privacy leakage makes evidence providers hesitant about sharing personal trust evidence. On the other hand, lacking sufficient evidence will influence the accuracy of trust evaluation. Therefore, it is important to guard privacy in trust evaluation in order to guarantee fast development of trust management.

Existing work related to Privacy-Preserving Trust Evaluation (PPTE) is rare and imperfect. Most existing methods of trust evaluation did not consider privacy preservation [2–11]. They generally aggregated plain trust evidence to calculate a trust value directly. In order to preserve the privacy of evidence providers, it is preferred that the collected evidence is encrypted and processed in an encrypted manner and the final evaluation result can only be accessed by authorized parties. But in this kind of methods it is hard to detect malicious evidence providers and thus filter their contributions during trust evaluation since the evidence is encrypted. Therefore, the accuracy of trust evaluation becomes difficult to be ensured. Recent advances in privacy-preserving aggregation have mainly been performed in the areas of wireless sensor systems and smart metering [12–19]. These methods cannot be directly applied into trust evaluation due to the difference of system or security models. Most existing work focused on resisting outsider-only attacks, while internal attacks raised by malicious evidence providers were not seriously considered. Recent research started to pay attention to the privacy issue of trust evaluation [20–28], but with limitations on generality, efficiency and reliability. This makes practical deployment of these solutions very difficult and further study is therefore highly needed. Moreover, most privacy-preserving aggregation schemes [12–19] focus on aggregating collected data for a designated requesting party. This fact makes them impossible to be applied into such a scenario that the aggregated data is requested by a number of different parties due to high computation and communication costs. How to share the aggregated evidence among authorized requesters in a secure and effective way is still an open issue.

We are still facing a number of challenges for PPTE. First, many traditional and existing trust evaluation methods cannot be applied if privacy preservation should be suppored. Second, accuracy and reliability of trust evaluation could be lost when privacy preservation has to be supported. It becomes very difficult to overcome internal attacks raised by malicious evidence providers. Third, reducing computation complexity becomes a challenge, especially when cryptographic technologies are applied. PPTE based on big data is hard to be supported with sound efficiency. Forth, flexibly controlling access to evaluation results for multiple authorized parties with computation efficiency has not been well solved. Finally, generality has not been seriously investigated for the purpose of supporting various trust evaluation theories and at the same time preserving privacy for all involved entities.

1.2. Main contributions

In this paper, we propose two schemes to preserve privacy in trust evaluation. To reduce the communication and computation costs, we propose to introduce two servers to realize the privacy preservation and evaluation result sharing among various requestors. We consider a scenario with two independent service parties that do not collude with each other due to their business incentives. One is an Authorized Proxy (AP) that is responsible for access control and management of aggregated evidence to enhance the privacy of entities being evaluated. The other is an Evaluation Party (EP) (e.g., offered by a cloud service provider) that processes the data collected from a number of trust evidence providers. The EP processes the collected data in an encrypted form and produces an encrypted trust pre-evaluation result. When a user requests the pre-evaluation result from EP, the EP first checks the user's access eligibility with AP. If the check is positive, the AP re-encrypts the pre-evaluation result that can be decrypted by the requester (Scheme 1) or there is an additional step involving the EP that prevents the AP from obtaining the plain pre-evaluation result while still allowing decryption of the pre-evaluation result by the requester (Scheme 2). In either case, the requester then finishes the trust evaluation by itself by decrypting the pre-evaluation results, aggregating and processing them together with evidence statistics recorded by EP and potentially also the evidence accumulated locally.

A homomorphic encryption technology, concretely additive homomorphism is applied to realize trust pre-evaluation at EP based on encrypted data collected from a number of trust evidence providers. Considering the current technical limitations of fully homomorphic encryption and its high computational complexity, our schemes attempt to achieve both efficiency and privacy preservation by conducting partial trust evaluation at a third party (e.g., EP) that cannot be fully trusted and is curious on privacy. Meanwhile, we propose two algorithms of trust evaluation in order to illustrate how the proposed two schemes can support PPTE in different trust evaluation cases. The illustrated cases contain evidence summation and achieve reliability in trust evaluation by minimizing the impact of attacks raised by malicious evidence providers. Specifically, the contributions of this paper can be summarized as below:

- We show how to preserve the privacy of trust evidence providers by proposing two security schemes for PPTE in order to encourage trust evidence provision.
- We propose two algorithms of trust evaluation that can flexibly support the implementation of the two PPTE schemes in different situations. Both algorithms exhibit the characteristics of trust and resist several typical internal attacks, which is verified through simulations.
- We prove the security and justify the performance of two PPTE schemes through analysis and implementation. Through comparison, we show the pros and cons of the schemes and their proper application scenarios.
- We show that our schemes are suitable in the world of big data. They can be applied in various scenarios with either a small or big number of evidence providers.

The rest of the paper is organized as follows. Section 2 gives a brief overview of related work. Section 3 introduces the system and threat model and our design goals, followed by detailed descriptions of two schemes and trust evaluation algorithms in Section 4. Section 5 gives security analysis and performance evaluation. The application scenarios are presented in Section 6. And finally we conclude the paper in the last section.