Journal of Computational Science 26 (2018) 87–107

Contents lists available at ScienceDirect

Journal of Computational Science

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

A privacy-preserving mobile application recommender system based on trust evaluation

Kun Xu [a], Weidong Zhang [b], Zheng Yan [a,c,*]

[a] The State Key Laboratory on Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an 710071, China
[b] The State Key Laboratory on Integrated Services Networks, School of Telecommunications Engineering, Xidian University, Xi'an 710071, China
[c] Department of Communications and Networking, Aalto University, Espoo 02150, Finland

ARTICLE INFO

Article history:
Received 23 December 2017
Received in revised form 9 February 2018
Accepted 1 April 2018
Available online 3 April 2018

Keywords:
Recommender system
Mobile application
Privacy protection
Homomorphic encryption

ABSTRACT

Too many mobile applications in App stores results in information overload in App market. Mobile users are confused in choosing suitable and trustworthy mobile applications due to a large number of available candidates. A mobile application recommender system is a powerful tool that helps users solve this problem. However, there are few feasible recommender systems focusing on recommending mobile applications in the literature. First, few researches study user trust behavior based recommendation on mobile applications. Second, the accuracy and personalization of existing recommender systems need to be further improved. Particularly, privacy preservation is still an open issue in mobile application recommendation. In this paper, we propose two privacy-preserving mobile application recommendation schemes based on trust evaluation. Recommendations on mobile application are generated based on user trust behaviors of mobile application usage. In these two schemes, user private data can be preserved by applying our proposed security protocols and utilizing homomorphic encryption. We further implement two schemes and develop two mobile Apps that can be applied in different scenarios, i.e., a centralized cloud service and distributed social networking. Security analysis, performance evaluation and simulation results show that our schemes have sound security, efficiency, accuracy, and robustness.

1. Introduction

Mobile devices have become an inseparable part of people's daily life nowadays. We are now living in a world with full support of the mobile Internet. Mobile users can do many things that are essential in their routine lives with the help of mobile applications, e.g., taking photos, enjoying entertainments, playing games, surfing web sites, taking a free riding, shopping online, social networking, reading news, consuming banking services, performing mobile payment, checking personal health, and so on. Mobile application based services have provided unbelievable convenience to mobile users, thanks to the smart phones that can access to the Internet at any time and in any places [12]. As an interface of operating smart phones, mobile applications installed in smart phones allow mobile users to enjoy various mobile Internet services and personal applications.

Mobile applications are software packages that can be executed in mobile devices [1]. To satisfy various needs of mobile users, large numbers of mobile applications are developed by manufacturers or third-party developers [2]. Fierce competitions among them result in a fact that there are so many applications with similar functions in the market, which make mobile users confused when choosing suitable applications for personal use. This is a typical phenomenon of information overload.

A recommender system is an effective tool that can be utilized to solve the problem of information overload [3,4]. A mobile recommender system is a system of generating recommendations for mobile users in a mobile Internet environment [5]. Several kinds of recommendation methods, e.g., collaborative filtering, content-based filtering and hybrid approaches [6,7], have been researched for generating recommendations in certain fields (e.g., music, movie, etc.) based on user personal profiles that mostly contain sensitive and private user information. Privacy leakage may arise without protection on data privacy and identity privacy [8,9].

1.1. Motivation

Proper selection of good applications can provide sound usage experiences to mobile users by offering high quality mobile Internet

* Corresponding author at: The State Key Laboratory on Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an 710071, China.
E-mail addresses: wdzhang@xidian.edu.cn (W. Zhang), zyan@xidian.edu.cn (Z. Yan).

https://doi.org/10.1016/j.jocs.2018.04.001

services. User wide acceptance also impacts the success of mobile applications. However, too many mobile applications available in the mobile app market makes mobile users confused in applications choose for their personal use [10,7,11,12,1,4]. Some mobile applications request for excessive permissions beyond necessary and collect unnecessary information from a user, which may impact user privacy without user attention [13–16]. With the help of a recommender system, recommendations on good and credible mobile applications can be generated for users so that they can get to know applications with high quality. Although recommender systems are widely used nowadays [6,3,17], little research work has been done with regard to mobile application recommender system. A common phenomenon is that mobile users trend to download applications that have high rating scores or download numbers from mobile app stores [11,12]. But the rating score or the download number cannot ensure that an application is good enough or sufficiently suitable for a user, especially when the score or the download number cannot accurately reflect the real quality or expected quality of users. Some existing studies evaluate the quality of an application and recommend applications based on trust, or functional behaviors of applications [18,19,10,11,20,21]. But they ignore a fact that the trust behaviors of mobile users when they consume applications can greatly imply user preferences and thus offer valuable information for application recommendations. The trust behavior is a user's actions to depend on an application or believe the application could perform as expectation, e.g., use an application regularly and continue consuming the application even facing some small problems [1]. The recommendation generated based on user trust behaviors becomes more accurate and personalized than other methods that analyze applications themselves.

However, existing mobile application recommender systems rarely take privacy preservation into concern [22,18,19,10–12,1]. User sensitive and private data are normally collected and computed when generating recommendations. In this case, privacy protection becomes important for mobile users [4,5,9,23–26]. Our previous work named TruBeRepec [1] generates mobile application recommendations based on user trust behaviors, which results in the improvement of accuracy and personalization of recommendations. Although TruBeRepec can protect user privacy to some extent by pre-processing user trust behavior data at mobile phones before sharing them with a reputation service provider, this approach cannot protect user behavior privacy with high security. A better solution is expected.

We can find some work about privacy-preserving recommendation [27,8,28–30,17,31–36]. The literature explored privacy protection and security methods from several aspects, such as trust transmission, social relationships, laws and policy, and cryptographic methods. However, existing schemes or methods cannot be directly applied into or not suitable for mobile application recommender systems due to the different context of mobile applications. How to protect user privacy while generating accurate and personalized recommendations on mobile applications based on user trust behaviors is still an open issue.

We are still facing a number of challenges to achieve a privacy-preserving mobile application recommender system. First, many private data of users are collected by the recommender system and how to control the size of data to reduce communication and processing costs is a crucial task when we design a mobile application recommender system. This issue is rarely considered in existing work. Second, how to ensure user privacy with sound security by resisting a number of attacks on the recommender system is another challenge. Finally, a successful design should be demonstrated by real implementation and performance tests. But introducing privacy protection by applying cryptographic techniques could worsen system performance, e.g., efficiency. How to make the recommender system perform efficiently in mobile devices with limited resources and achieve user acceptance is still a practical challenge.

1.2. Main contributions

In this paper, we propose two privacy-preserving mobile application recommendation schemes. The two schemes are based on our previous work named TruBeRepec [1]. We improve it by designing two privacy-preserving mobile application recommender schemes with different system structures and different operation procedures, so that they can be applied into different application scenarios. Concretely, one scheme is a privacy-preserving mobile application recommender system for cloud services, namely PPMARS-C. This scheme is a centralized recommender system that involves three kinds of system entities: mobile devices (MDs) that provide the data of user trust behaviors in terms of mobile application usage. The MD can be a smart phone for example; a cloud Service Provider (SP) that collects, stores, and processes user data for generating privacy-preserving recommendations. SP can be a cloud server with powerful storage ability and computational capability; a Privacy Center (PC) that provides necessary functionalities for data protection and user authentication. PC can be played by a certificate authority, for example. PPMARS-C is suitable for being applied in a cloud service environment.

Another scheme is a privacy-preserving mobile application recommender system in social networks, namely PPMARS-S. This scheme is a distributed recommender system that involves two kinds of system entities. One is mobile device (MD) that communicates with other devices and provides user data of trust behaviors in terms of mobile application usage. The MD can be a smart phone. The other kind of entities is a Service Provider (SP) that communicates with a certain number of MDs and generates privacy-preserving recommendations. The SP can be a base station or an edge device with sufficient computational capability. PPMARS-S is suitable for being applied into social networks in a distributed environment.

In order to improve the accuracy and personalization of recommendations, the mobile application recommendations in both schemes are generated based on the data of user trust behaviors of using mobile applications installed in their mobile devices. In order to preserve user privacy in both schemes, anonymity, public key encryption, and homomorphic encryption technology, concretely additive homomorphic encryption, and other technologies are utilized to guarantee identity security, data transmission security, and data processing security. We attempt to achieve effective, accurate, and robust recommender systems. Meanwhile, we develop two Android Apps that implement the proposed two schemes. We conduct performance evaluation by running two recommender systems and make a survey about user experiences in a real usage environment. Specifically, the contributions of this paper can be summarized as bellow:

- We propose two privacy-preserving mobile application recommendation schemes that can generate recommendations on mobile applications while preserve user privacy. The two schemes have different system structures and operation procedures so that they can be used in different application scenarios.
- We prove the security and evaluate the performance of the proposed schemes through analysis and implementation. By running the implemented recommender systems in a real context and making comparison with existing work, we show the efficiency and effectiveness of our schemes.
- We evaluate robustness of the proposed two schemes with regard to several typical attacks through simulations. The result further