# Accepted Manuscript

ARMOR: A trust-based privacy-preserving framework for decentralized friend recommendation in online social networks

Xindi Ma, Jianfeng Ma, Hui Li, Qi Jiang, Sheng Gao

PII: S0167-739X(17)30054-7
DOI: https://doi.org/10.1016/j.future.2017.09.060
Reference: FUTURE 3716

To appear in: *Future Generation Computer Systems*

Received date : 12 January 2017
Revised date : 25 May 2017
Accepted date : 22 September 2017

Please cite this article as: X. Ma, J. Ma, H. Li, Q. Jiang, S. Gao, ARMOR: A trust-based privacy-preserving framework for decentralized friend recommendation in online social networks, *Future Generation Computer Systems* (2017), https://doi.org/10.1016/j.future.2017.09.060

# ARMOR: A Trust-based Privacy-Preserving Framework for Decentralized Friend Recommendation in Online Social Networks

Xindi Ma[a,*], Jianfeng Ma[a], Hui Li[a], Qi Jiang[a,b], Sheng Gao[c]

[a]*School of Cyber Engineering, Xidian University, Xi'an, China*
[b]*School of Computer & Software, Nanjing University of Information Science & Technology, Nanjing, China*
[c]*School of Information, Central University of Finance and Economics, Beijing, China*

**Abstract**

Friend recommendation in online social networks (OSNs) has recently experienced rapid development and received much research attention. Existing recommender systems on the basis of the big social data mostly employ centralized framework, which would cause lots of problems, such as single point failure, communication bottleneck and so on. Some other studies focus on decentralized framework for recommendation, however, most of them concentrate on the improvement of recommendation quality, while underestimating privacy issues, e.g. OSN users' privacy concerns regarding their social relationships, social attributes, and recommendation profiles. In this paper, we propose a novel decentralized framework, namely ARMOR, which utilizes OSN users' social attributes and trust relationships to achieve the friend recommendation in a privacy-preserving manner. In ARMOR, we adopt a light-weight privacy-preserving protocol to aggregate the utilities of multi-hop trust chains and compute the recommender results securely. We also analyze the efficiency of ARMOR in theory and prove that OSN users' privacy can be preserved. Finally, we conduct an experiment to evaluate ARMOR over a real-world dataset and empirical results demonstrate that our ARMOR can effectively and efficiently recommend friends in a privacy-preserving way.

*Keywords:* Friend recommendation, online social network, privacy preservation, trust.

## 1. Introduction

With the rapid development of information technology and the proliferation of online social interactions, we are witnessing a widespread popularity of Online Social Networks (OSNs). Similar to what people usually do in real life, OSN users always try to extend their social circles in order to satisfy various social demands, e.g., leisure, business, science, and so on [1].

Friend recommendation is essential for users to enlarge their social circles in OSNs. According to the recommendation model, friend recommendation can be classified into two categories: social graphs based, like friends of friends (FoFs); or big social data based, like tags and blog posts [2]. However, the recommender system based on big social data is always centralized, where a service provider is included and may cause the problems of single point failure and communication bottleneck. What's worse, these recommendations also ignore the social influence, like trust, which is a key driver in motivating users to establish friendships [3].

Sharma et al. [4] found that recommendation algorithms based on FoFs method performed no worse than those based on the full network, even though the FoFs-based recommendation required much less data and computational resources. And we consider that it is more probable a person will know a friend of his friends rather than a random person [5]. So the decentralized friend recommender systems based on the FoFs can provide more valuable recommendations while consuming less resources. However, the decentralized recommender systems also face another common problem, namely, privacy. For instance, if we want to look for a cardiologist over some professional OSNs, such as PatientLikeMe [1], for helpful suggestions and preliminary diagnosis. Without a privacy-preserving mechanism, requesting the recommendation from non-close friends or strangers not only reveals our profiles, but also discloses our private information, such as health conditions and medical information. Even worse, the recommendation approaches [6, 7] which apply identity to recommend strangers will disclose OSN users' social relationships to the public, which impede users from utilizing it, and also decrease the possibility of establishing the multi-hop trust chain if one of OSN users on the chain returns a negative result. Therefore, it is crucial to protect user privacy when utilizing the friend recommendation in OSNs. Unfortu-

*Corresponding author
*Email addresses:* xdma1989@gmail.com (Xindi Ma), jfma@mail.xidian.edu.cn (Jianfeng Ma), hli@xidian.edu.cn (Hui Li), jiangqixdu@gmail.com (Qi Jiang), sgao@cufe.edu.cn (Sheng Gao)

[1] http://www.patientslikeme.com/