IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Friend Discovery Mechanism with Secure Communication and Accurate Recommendation for Social Web Networks

Prof. Neha Pharande[1], Sailen Raj[1], Ranoo Khatri[1], Krishna Sawalkar[1], Karan Mahesh[1]

Department of Computer Engineering, Sinhgad College of Engineering, Pune, India[1]

Abstract: Nowadays, online social networks is a very popular communication platform, using on awide range of applications. Social networking sites employ recommendation systems in contribution to providing better user experiences. Existing social networking services recommend friends to users based on their social graphs, which may not be the most appropriate to reflecta user's preferences on friend selection in real life.We propose, a novel semantic-based friend recommendation system for social networks,which recommends friends to users based on their life styles instead of social graphs. Novelsemantic approach measures the similarities of two members based on information containedin their profiles and recommends friends to users if their life styles have high similarity. Comparison Analysis Algorithm helps in securing the users data from visualizing to others. It alsohelp users to choose accurate friend requests by checking the matching percentage value.The results show that the recommendations accurately reflect the preferences of users inchoosing friends. This system can be used in finding accurate and secure recommendationsin social networks. Results of this system represent strong potential for developing link recommendation systems using this combined approach of personal interests and the underlyingnetwork.

Keywords: social networking services, friend recommendation, graphs, novel semantic, Comparison Analysis Algorithm.

I. INTRODUCTION

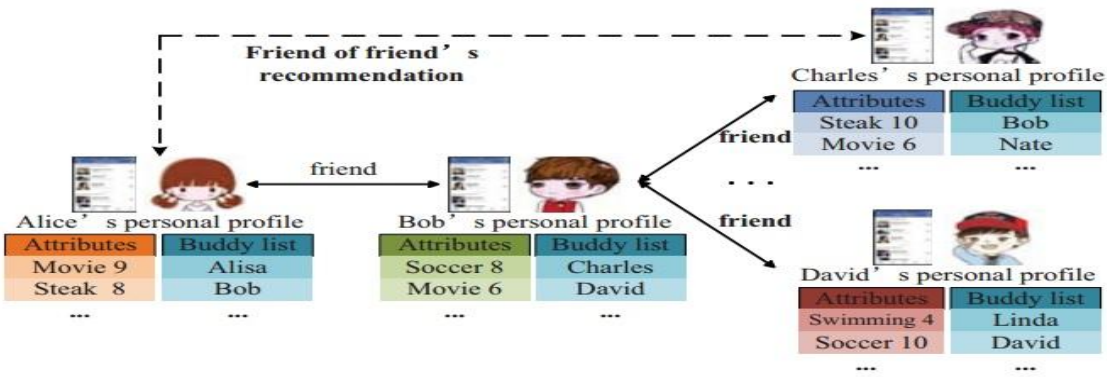
Nowadays social networking services recommend friends to usersbased on their social graphs, which may not be the most appropriate to reflect a user's preferences on friend selection in real life. User may release some personal information, which may raise serious privacy concerns .To resolve this, we design friend-of-friend's recommendation using secure and accuratefriend discovery for privacy-aware user by similarity measure technique.Novel semantic approach measures the similarities of two members based on information contained in their profiles and recommends friends to users if their life styles have high similarity. ComparisonAnalysis Algorithm helps in securing the users data from visualizing to others. It also help users to choose accurate friend requests by checking the matching percentage value.

II. SIMILARITY FUNCTION

A Similarity function quantifies the similarity between two objects. It take on large values for similar objects and either zero or a negative value for very dissimilar objects. It is a priority-aware similarity function based on the Dice Similarity coefficient considering the common attributes with their priority.

Similarity function considers both the number of common attributes and the corresponding priorities, as well as the ratio of matched attributes over all the inputs.Dice similarity coefficient is represented as

$$\frac{2|A' \cap B'|}{|A'|+|B'|} \in [0, 1].$$



DOI10.17148/IJARCCE.2017.63114

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

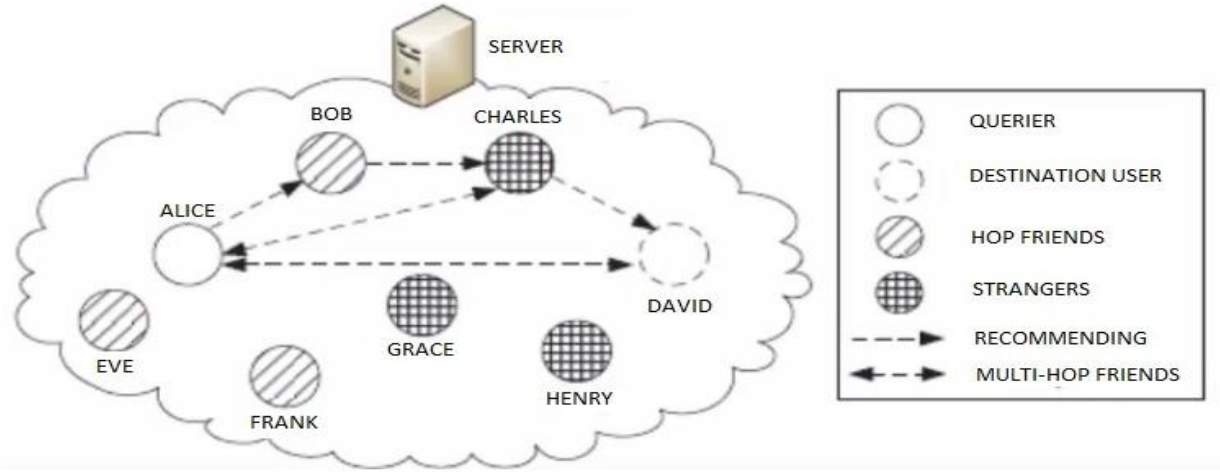
Here A and B is the attributes with their priority. The range of the priority-aware similarity is from 0 to 1, in which 0 represents "no common interest at all" 1 indicates "the same interest with the same priority".

III. FRIEND DISCOVERY

Friend discovery phase is discovery of potential friends in vicinity and prepare for coming friend recommendation phase.

Here, all the friends which were discovered by similarity function is further filtered to discover accurate friend.

Hash function is applied to set of attributes and secret key is choose in randomly order for the attributes of the discovered friend. It is then broadcasted with the matching request.



IV.FRIEND RECOMMENDATION

Friend recommendation phase is the friend of friend discovery with no loss of accuracy. Friend recommendation is achieved properly and automatically on user's friend side.

Friend is automatically discovered and recommended to the user comparing the attributes of the different entities mentioning their interest with their priority. It recommend most appropriate friend reflecting the user's preferences on friend selection in real life.

V. SECURITY ANALYSIS

Some of the users have privacy concern for their personal information. For such privacy aware user friend is recommended in such a way that the system don't release any privacy information of the users. Security is important factor in case of information. Many of existing schemes employ tools to guarantee security and privacy properties, but it is hard to keep a balance security and efficiency.

After discovering the accurate friend, it is recommended to the user using the combination of commutative encryption function and bilinear pairing. The commutative encryption function is typically described in the setting of the multiplicative group of the integers modulo a prime. It can be modified to work in the group of elliptic curve. Bilinear pairing is the use of a pairing between elements of two cryptographic groups to a third group with a mapping.The security and performance is thoroughly analysed. Commutative encryption is not enough to keep recommendation system secure.

To make it secure enough so that user cannot learn anything from the inputs except the recommended friend, recommendation is done in simulation in which the obtained information cannot be distinguished. Below figure shows security phase using commutative encryption in simulated environment for friend recommendation.

VI. SYSTEM ARCHITECTURE

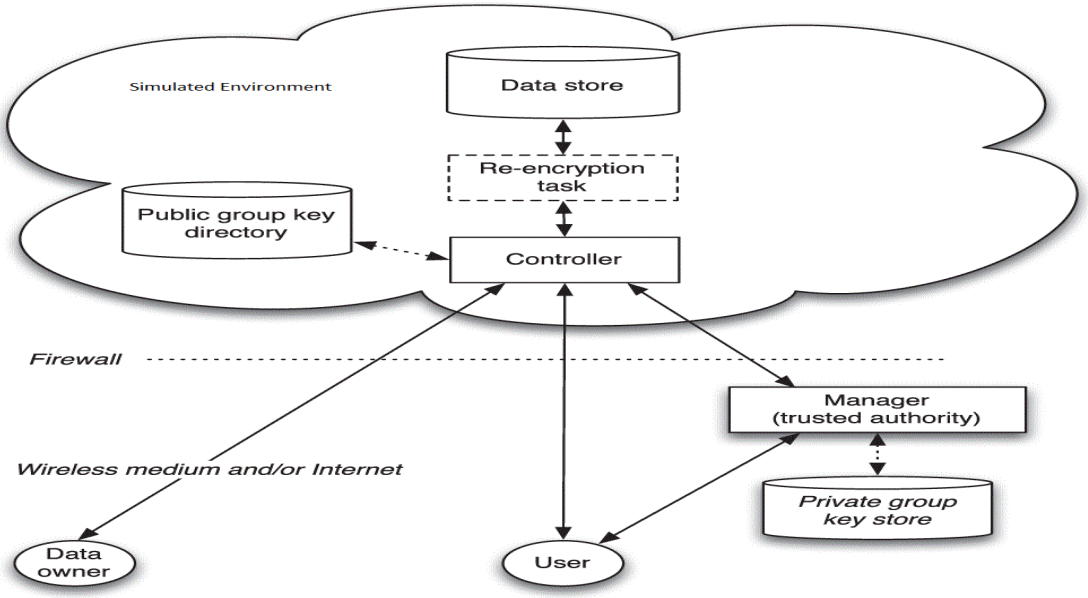
The scheme implemented allow users to enlarge their own social community based on the friend of friend recommendations privately. The user can communicate with others in the vicinity via some short range techniques such as Wi-Fi or Bluetooth. Every users has their personal profile, including many attributes and a buddy list. There may be situation like when user come into a place (i.e. a new company or school) for the first time, and is quite interested in finding more friends in common.

One of the user friends, who has his own profile and set of friends, can recommend friend to that useronce they have more common interests, especially with similar priorities. To achieve this goal, similarity function is constructed, which is employed in the friend discovery phase to measure the similarities with other users.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017



VII .CONCLUSION

To discover a secure and accurate friend, we proposed a friend of friend recommendation system. We first exploited a similarity function based on the Dice similarity, considering the number of common attributes, the corresponding priorities and the ratio of the matched attributes over all the inputs to avoid insider attacks. Then we designed a secure friend recommendation phase, with carefully combining the commutative encryption function and bilinear pairings, to provide users more opportunities to know potential friends from the existing friend's recommendations.

REFERENCES

1) HTTPS://EN.WIKIPEDIA.ORG/WIKI/SIMILARITYMEASURES.
2) https://eprint.iacr.org/2008/356.pdf
3) https://en.wikipedia.org/wiki/Three-pass_protocol
4) https://en.wikipedia.org/wiki/Pairing-based_cryptography.
5) Coding theory, cryptography and related areas.Johannes Buchmann, Tom Hoeholdt, Henning Stichtenoth, Horacio Tapia Recillas.
6) B. Niu, Y. He, F. Li, and H. Li, "Achieving secure friend discovery insocial strength-aware pmsns," in Proc. of IEEE MILCOM 2015.
7) Yuanyuan He, Fenghua Li, Ben Niu and JiafengHua"Achieving Secure and AccurateFriend Discovery Based on Friend-of Friend's Recommendations", in Proc. Of IEEE ICC2016.
8) Agrawal, R., Evfimievski, A., and Srikant, R., "Information sharing across privatedatabases,"International Conference on Management of Data (ACM SIGMOD),ACMPress, 2003.
9) O. Goldreich, "Secure multi-party computation," Cryptography andIntractability, vol. 2, no. 3, pp. 927–938, 2002.
10) F. Li, Y. He, B. Niu, H. Li, and W. Hanyi, "Match-more: An efficientprivate matching scheme using friends-of-friends recommendation," inProc. of IEEE ICNC 2016.
11) M. Li, N. Cao, S. Yu, and W. Lou, "Findu: Privacy-preserving personalprofile matching in mobile social networks," in Proc. Of IEEE INFOCOM 2011