International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

SPFM : Scalable and Privacy-Preserving Friend Matching in Cloud

Mohini Dumre, Nilima Dhok, Sonal Ramteke
Nagpur University, Nagpur, Maharashtra, India

ABSTRACT

Profile data, interest, and mobility matching is more than important for fostering the wide use of social networks. The social networks such as Facebook, Line, or WeChat recommend the friends for the users based on users personal data such as common contact list or mobility traces. Here, users' personal information to the database for friend matching will raise a serious privacy concern due to the potential risk of data abusing. In this paper, we propose a novel scalable and privacy-preserving friend matching protocol, which aims to provide a scalable friend matching and recommendation solutions without revealing the users personal data to the cloud. The various from the previous works which have multiple number of protocols, it presents a scalable solution which can prevent honest and curious cloud from obtaining the original data and support the friend matching of multiple users simultaneously. The detailed feasibility and security analysis on it and its accuracy and security have been well demonstrated via extensive simulations. The result show that our system works even better when original data is large.

Keywords: Profile,Social Network,WeChat, SPFM ,Cloud.

I. INTRODUCTION

Social networking is grouping of individuals into specific groups. Social media is a wide range of internet based and services that allow users to participate in online communities. It is also a platform to built social relations between people who share similar interests, activities, backgrounds and real life connections. Social media also allows individuals, companies, organizationsand governments to interact with a lot of people. There are number of websites focus on particular interests which means anyone can be a member, but it does not matter what their hobbies or interests are. Once you are member of community you can be friends with similar interests and can unfriend those friends.

What is meant by Social Network?

Social Networking is networking where individuals with similar interests connect with each other by using their phone. The present trend for social networking websites is to create applications to give real time access and user instant from the particular device. Face to face interaction plays an important role in our day to day life, especially for social networking purposes the initiator and its matching user directly find out and connect to each other, without knowing anything about other users profile attributes, making new connections according to personal preferences to matching user profile is an important task, while the rest of the users should also know nothing about the two users matching attributes. The web based social networks is extended for access through browsers and smartphone applications.

II. LITERATURE SURVEY

In existing system for such services, usually all users directly publishes their complete profile for other people to search. In many applications, the user's

profile may contain personal information which are sensitive and which they doesn't want to make public. The present system addresses the verifiable privacy preserving profile matching and secure communication .The profiles of all participants, should not be exposed without their consents and can reduce the barrier to participate in Social Network. The two techniques used are Private Set Intersection (PSI) and Private Cardinality of Set Intersection(PCSI). Disadvantages Possibility for hackers to launch spam and virus attacks. Increases the risk of people being victim to online scams that seems original,resulting in the theft of data and the identity. It also results in the productivity loss, especially if the employees are busy in updating their profiles

Proposed System

Treat the user's profile as multiple attributes chosen from a public set of attributes provide well designed protocols to privately match user's profiles based on the private vector dot product. In the proposed system, the AES is used to enhance the security of the files. Here the profiles of two users are taken as two matrices and the attributes such as location and hobbies of the each user which is written in their profiles are compared using private vector dot product. After the comparison of the attributes we can find the similarities of two profiles and thus we can send and accept the request. The files that we need to share should be secured, we can secure the files by the encryption and decryption of the path that the file stored by using Advanced Encryption Standard.Advantages User can get better suggestion of friends based on the profile matching technique. The secrity of the files is enhanced by AES.

III. MATERIALS AND METHODS

AES (Advanced Encryption Standard) algorithm:
AES is based on a principle called substitution permutation network. It is very fast in both the software and hardware. AES has a constant blog size of 128 bits and key size of 128, 192, or 256 bits [10]. AES is symmetric key algorithm. It operates on a \4x4 matrix of bytes, termed as the state. AES cipher is specified as a number of repetitions of transformation rounds that converts input plain text into the final output of the cipher text. The each round consists of several processing steps, including one that depends on encryption key. A set of reverse roundsare applied to transform cipher text back into the original plain text using same encryption key.

IV. IMPLEMENTATION AND EVALUATION

There are four modules that should be implemented and they are authentication, Find friend, Recommendation and Data recognition module. Authentication

In the authentication module we can register and login through the system using personal details. Admin and user are the two authentication modules. Admin is the main person to control all the user actions. The user can register and store all the data through the system. It is important when dynamic IP addressing is used for computers on the trusted network. user's identity can be proved through this.

Find Friend

In the find friend module user can find friend, send request, accept request etc. Friends are suggested according to their attributes such as location and hobbies.

Recommendation

Recommendation is a module in which system recommend users matching friend .It is based on similarities of mutual friends that are described in the profile attributes values. These values are taken as the entity values. The system will match the entity values of profiles. If the two profiles share some similar entity values then it result shows two person may know each other.

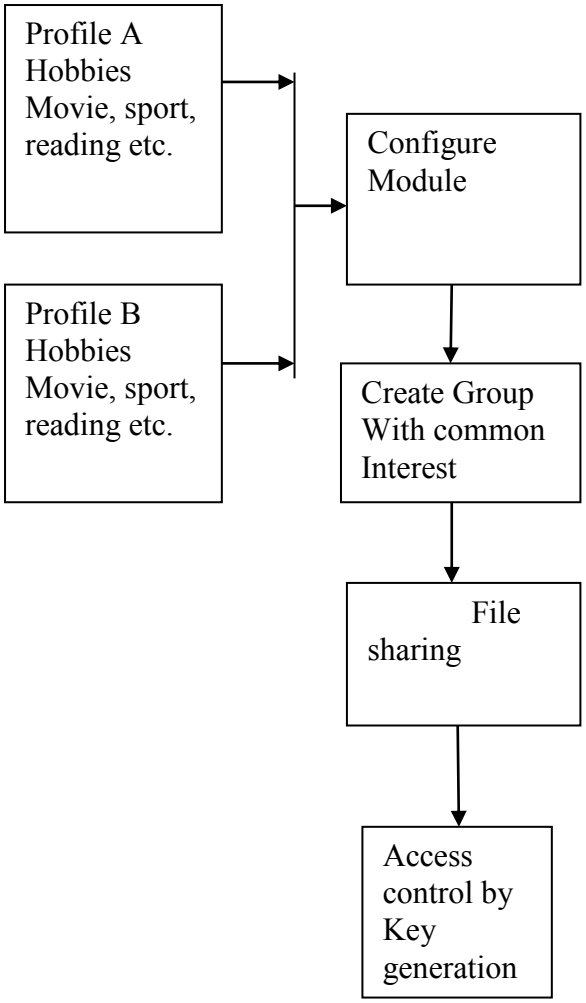

Figure1. System Model for Friend Discovery

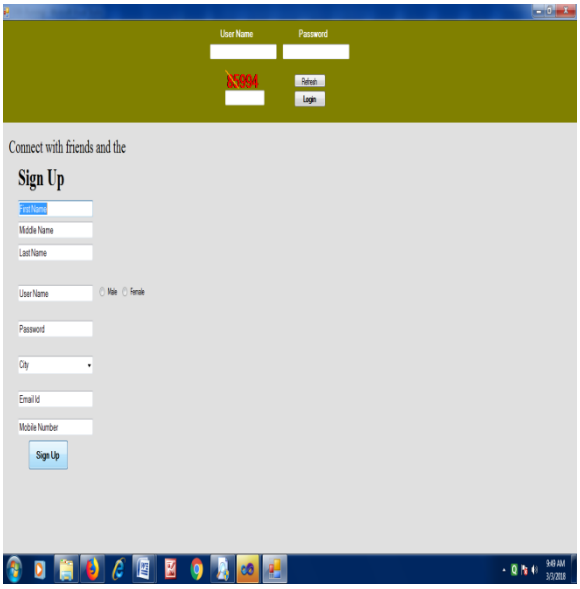

Figure2. Registration system

Data Recognition

In the Data recognition module the system request the details of the user to store and perform auto friend matching and analysis of the corresponding method.

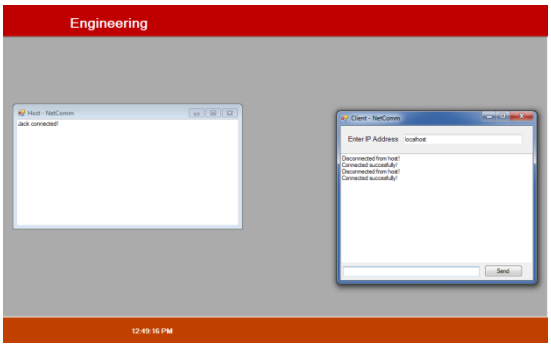

Figure 3. server interface model

AES (Advanced Encryption Standard) algorithm:

AES is based on a principle called substitution permutation network. It is very fast in both the software and hardware. AES has a constant blog size of 128 bits and key size of 128, 192, or 256 bits [10]. AES is symmetric key algorithm. It operates on a \4x4 matrix of bytes, termed as the state. AES cipher is specified as a number of repetitions of transformation rounds that converts input plain text into the final output of the cipher text. The each round consists of several processing steps, including one that depends on encryption key. A set of reverse roundsare applied to transform cipher text back into the original plain text using same encryption key.

V. CONCLUSION

In this paper we tackles the problem of conflicting phenomenon that arise from variety of cloud storage nowadays. The problem stems from the conflict bout exciting functions cloud providing and the potential security issues in cloud. Honest-but-curious server, cloud account loss or cloud attack all may lead to exposure of users' private data, which will be an irreversible disaster. Thus, we develop SPFM to achieve high accuracy matching while not expose accurate private data to cloud. We provide

VI. REFERENCES

[1]. A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," Science , vol. 347, no. 6221, pp. 509-514, 2015.

[2]. D. Lewis, "icloud data breach: Hacking and celebrity photos,"http://www.forbes.com/sites/davelewis/2014/09/02/icloud-data-breach- hacking-and-nude-celebrity-photos/.

[3]. R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y.Le Boudec, "Protecting location privacy: optimal strategy against local-ization attacks," inProceedings of the ACM conference on Computerand communications security ACM, 2012, pp. 617-627.

[4]. M. Li, N. Cao, S. Yu, and W. Lou, "Findu: Privacy-preserving personalprofile matching in social networks," inIEEE INFOCOM. IEEE,2011, pp. 2435-2443.

[5]. W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in social networks," in IEEE INFOCOM. IEEE, 2011, pp. 1647-1655.

[6]. J. He, M. Dong, K. Ota, M. Fan, and G. Wang, "Netseccc: A scalable and fault-tolerant architecture for cloud computing security,"Peer-to-Peer Networking and Applications, vol. 9, no. 1, pp. 67-81, 2016.

[7]. M. Dong, H. Li, K. Ota, L. T. Yang, and H. Zhu, "Multicloud-based evacuation services for emergency management,"Cloud Computing,IEEE, vol. 1, no. 4, pp. 50-59, 2014.

[8]. R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme withsymptoms-matching for mhealthcare social network," Networksand Applications, vol. 16, no. 6, pp. 683-694, 2011.

[9]. M. Von Arb, M. Bader, M. Kuhn, and R. Wattenhofer, "Veneta: Server-less friend-of-friend detection in social networking," inIEEEInternational Conference on Wireless and Computing.IEEE, 2008, pp. 184-189.

[10]. L. Kissner and D. Song, "Privacy-preserving set operations," inAdvancesin Cryptology-CRYPTO. Springer, 2005, pp. 241-257.