Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 6 (2017) pp. 1885-1892
© Research India Publications
http://www.ripublication.com

Trust Based Profile Matching On Secure Social Network

D.Dhayalan[*], B.Balaji, A.Francina and S.Abitha-Bi
Department Of Master of Computer Applications
Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi-62.

Abstract

Online Social Networking is a way to connecting people well-balanced. So more immensely large number of OSN sites are elevated at speed like a face book, WhatsApp, LinkedIn and so on. All the OSN sites have to engender singularity and apperception of each user, so we require to amass rudimental information`s like denomination, mail id, mobile number and other details for every user have to engender friends circle for more interactive conversation among more members. But in this system, every utilizer has some of the activities on probing friends and making them as friends, there is no discussion between user activities for guidance and make friends. Any user can view profile details of other persons. These are the main disadvantage of Previous System. To overcome from the above problem, this project is proposed. In proposed system, if any users want to engender friend request then sent a request with some of the activity listed, then this request received people can view the activity value at abaft the request information. If someone to operate as Friend for the requested person then accept the request, Otherwise, its reject the request. After accepting the friend request, then send profile key to new Friend and also older friends for viewing the profile. This profile key is also changed at every time when the user changing the profile. After When the user can also send a profile key.

Keyword: OSN, PrideU , SMC , Parameter inference algorithm

[*] Corresponding Author email: dhayalan@velhightech.com

1. INTRODUCTION:

PrideU: Profile Matching in Secure Multi-party Computation (SMC), Proximity-based on user discovery and key establishment are two major issues for the usability of our profile matching protocols. The user for the first time to formalize, the problem of privacy-preserving distributed profile matching in OSNs, and to propose two sensible schemes that may cause increasing levels of user privacy preservation. Virtually designing lightweight protocols, the utilizer can utilize Shamir secret sharing as the main secure computation technique, while the utilizer may propose to adscititious enhancements to lower the proposed schemes' communication. This inspires the group formation logic in our proposed proof-of-concept (PoC) prototype implementation described at length in this work. It is generally based on the concept of integrated centralized and distributed systems [1].With the growth of mobile devices and online social networks (OSNs), people can connect with each other ubiquitously anytime. Mobile Social Networks (MSNs) are the emerging trend in mobile technology that combines wireless communication and social networking. MSN inherits advantages of delay tolerant networks (DTNs) and opportunistic networks (Opp-nets) [2].

We showed that with an additional commitment round before final reconstruction specific type of "set inflation attack" can be easily prevented where a malicious user influences the final output in her favorable way by changing her shares after seeing others'.

Users can view the number of friend request will engendered by the system itself. In this list, an user who are all view this list then click and view particular person's whole information like name, mail id, mobile number, date of birth and other information`s without the permission of that particular person and also generate friend request without any strategies. So the request will be received by the user, can also accept or reject request without any knowledge.

It includes following modules:

- ✓ Private matching protocols
- ✓ Private set intersection
- ✓ Secure multiparty computation
- ✓ Comparison between two users
- ✓ Secrete sharing (photo and video)
- ✓ Report generation

2. RESEARCH METHOD

Private Matching Protocols:

In social networking sites, the single user can view all the details of the person who has an account in social networks without their knowledge. So, we were utilizing the private matching protocol to block the users who was not kenned to you. This protocol will let us the user to accept the friend request from the other user If the request is not accepted by the utilizer then the details of the utilizer will not be shown to the unknown person. The adversary tries to find out the interests or the pro- files of the other users during the profile matching process. [3]

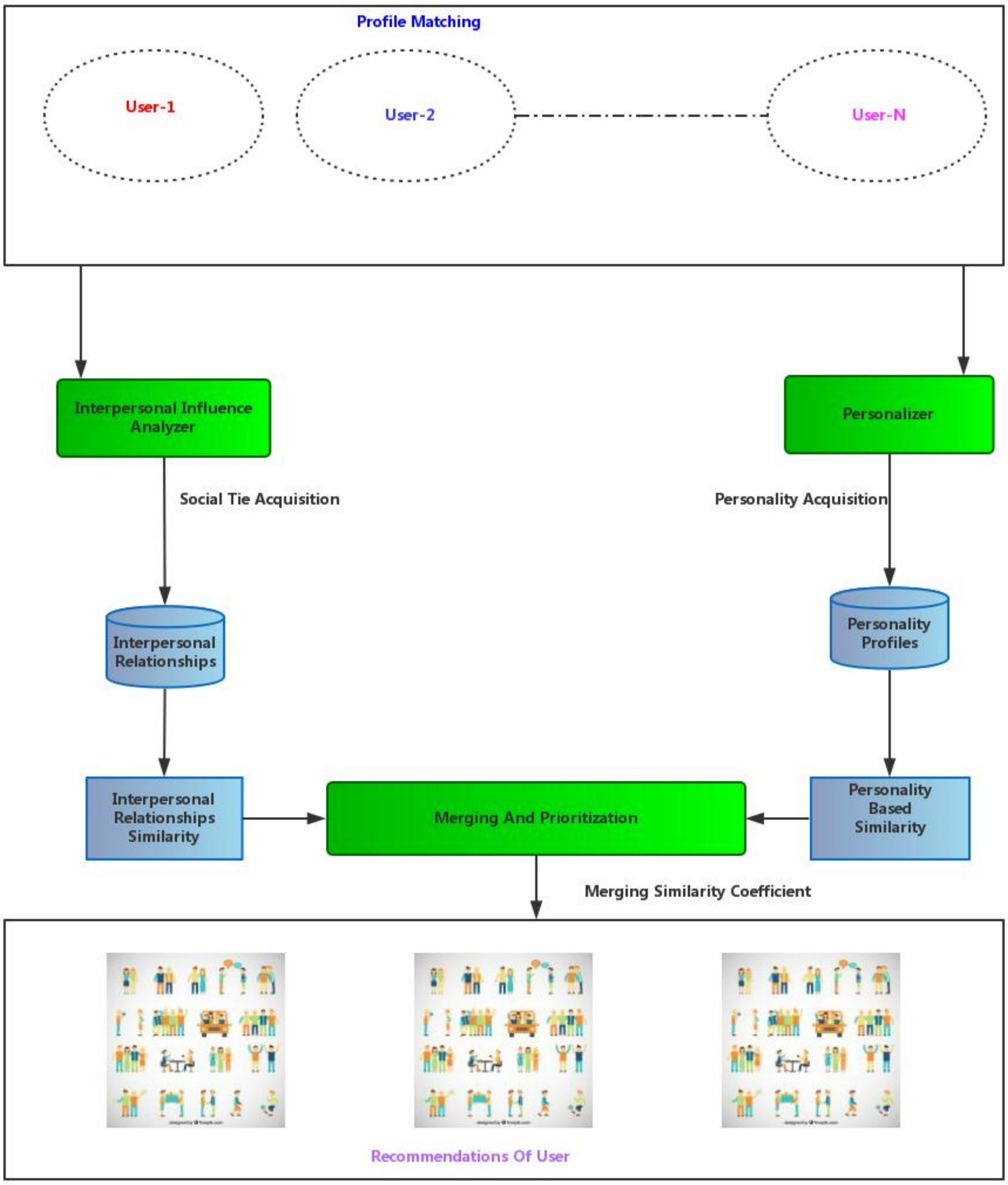

Profile Matching
User-1
User-2
User-N
Interpersonal Influence Analyzer
Personalizer
Social Tie Acquisition
Personality Acquisition
Interpersonal Relationships
Personality Profiles
Interpersonal Relationships Similarity
Merging And Prioritization
Personality Based Similarity
Merging Similarity Coefficient
Recommendations Of User

Figure 1. Architecture of Profile Matching

Private Set Intersection:

The private set intersection is utilized to evade the unknown person to view the profile details of an individual utilizer. Increasing dependencies on anytime-anywhere availability of data and the proportional increasing fear of losing privacy to motivate the need for privacy-preserving technique. The major implementation of this module is to intersect the details of each and every single. In OSN scenario, both OSN administrator and malicious users are potential attackers. Since it is usually the advertisers rather than users to pay for the OSN service, the interests of the advertisers might take priority of privacy protection for users [4], and OSN might be a potential attacker when considering the privacy protection of users.

Secure Multiparty Computation:

The secure multiparty computation is used to secure the user private details. If the user gave an access to the request send by the other user, then the user details can be viewed by the other parties. In this part, only a user can give access to the particular user based on his/her wish to view the profile details. It is a secure way for protecting the private information of the users.

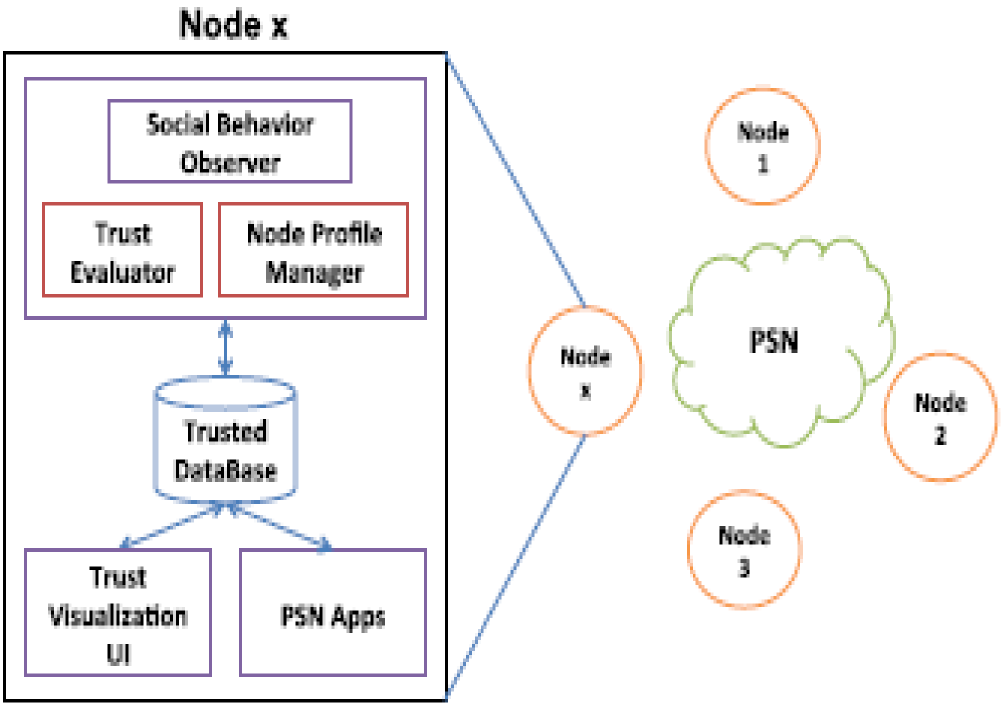
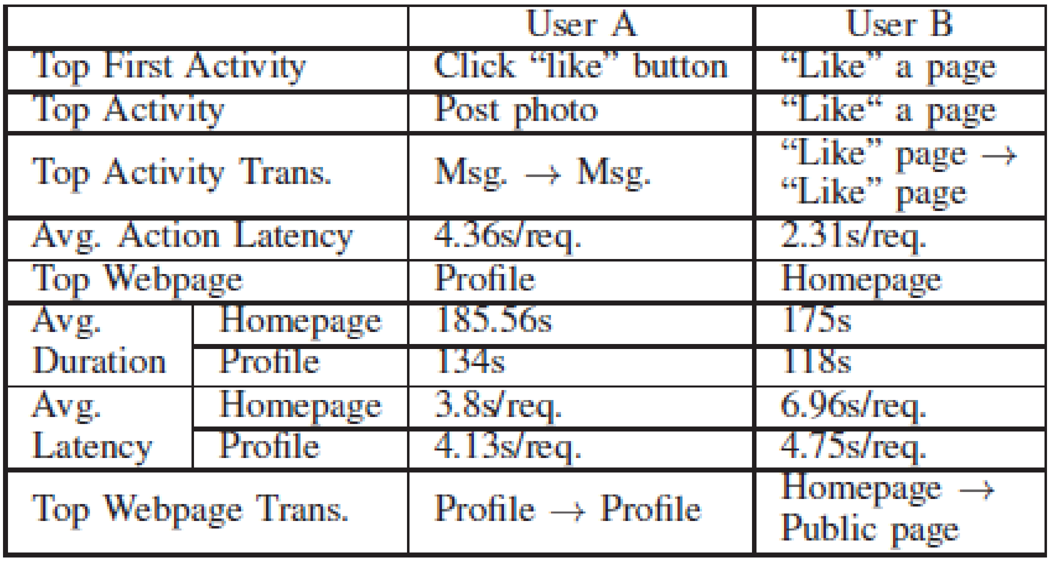


Figure 2. A System Model

Comparison between Two Users:

In social networking site the two user information can be compared and analyzed based on their interest and favorites. This is used to send request based on recommendation system. The comparison is purely based on the user interest in which the unknown individual user cannot able to view or access the personal and private information about user in a social networking site.

Table 1. Comparison between Two Users



		User A	User B
Top First Activity		Click “like” button	“Like” a page
Top Activity		Post photo	“Like“ a page
Top Activity Trans.		Msg. → Msg.	“Like” page → “Like” page
Avg. Action Latency		4.36s/req.	2.31s/req.
Top Webpage		Profile	Homepage
Avg. Duration	Homepage	185.56s	175s
	Profile	134s	118s
Avg. Latency	Homepage	3.8s/req.	6.96s/req.
	Profile	4.13s/req.	4.75s/req.
Top Webpage Trans.		Profile → Profile	Homepage → Public page

Secret Sharing (Photo and Videos):

We all know that the social networking site contains walls in which we post our videos, images and status which is not necessary to other user to view In secret sharing we can cull the utilizer for whom the videos and images should be reached or received so it engenders the privacy of the information.. This is applicable in group chats also. In group chat , if we have a ten members in a group but the images should be shared to only five members. In such a case the secret sharing method can be used.

Report Generation:

Admin generates the report based on the users account in social networking site. The report can contain all the details of the user regarding images, status, videos uploaded on the timeline or wall. This kind of details can be managed in the admin side report.

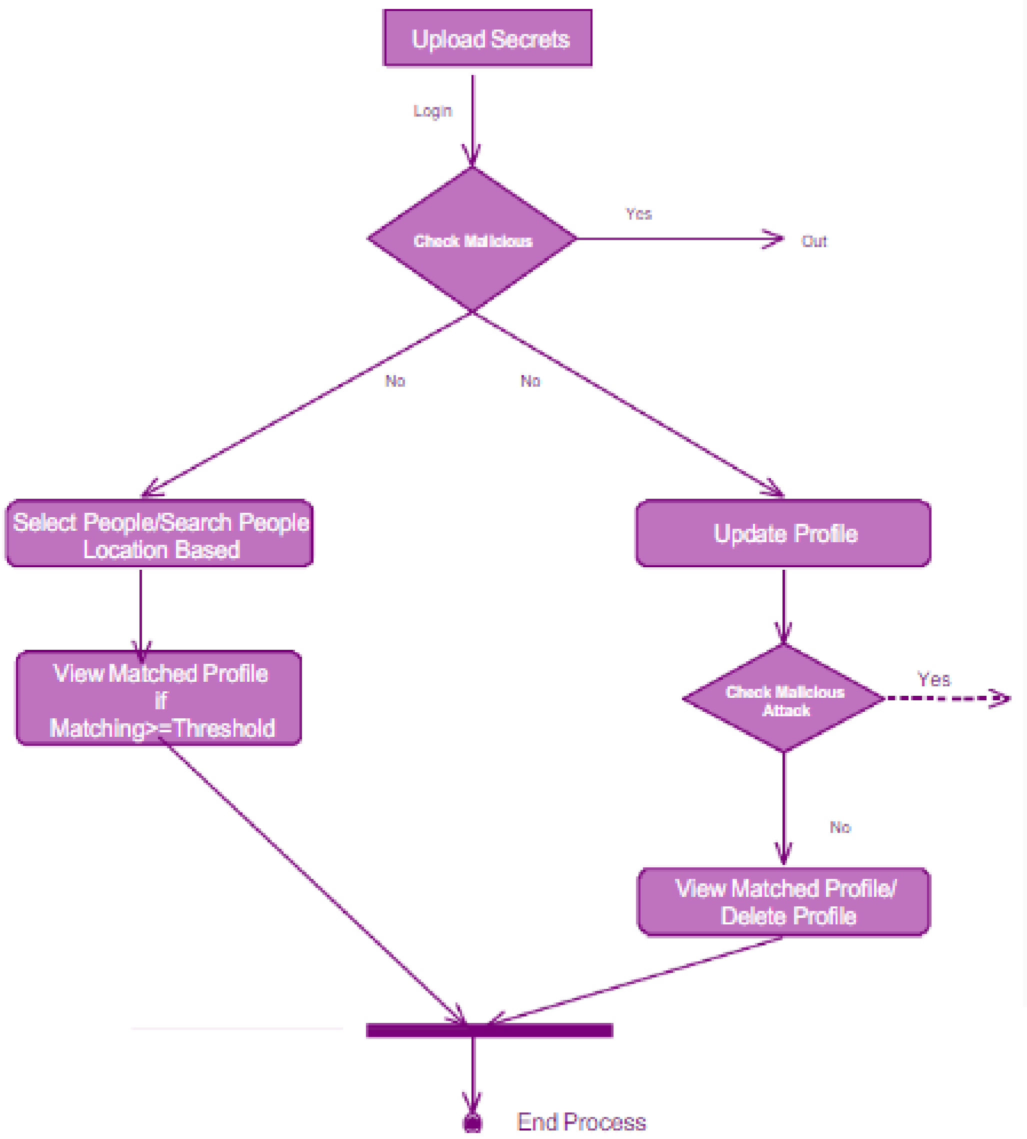

Upload Secrets
Login
Check Malicious
Yes
Out
No
No
Select People/Search People Location Based
Update Profile
View Matched Profile if Matching>=Threshold
Check Malicious Attack
Yes
No
View Matched Profile/ Delete Profile
End Process

Figure 3. ACTIVITY DIAGRAM OF PROFILE MATCHING

Algorithm 1: Parameter Inference Algorithm

Input:

Learning rate, regularization parameters,

Output:

Transform matrix A*u* for each user *u*,

Latent feature matrices U;V.

1: Initialize Au $\sim N(0; \mathrm{I}); \forall u$, U;V $\sim N(0; \mathrm{I})$

```
Repeat
    Uniformly draw a user $u$ from user set $U$
    Uniformly draw a repeat consumption of $u$ w.r.t. item
    $vi$at time $t$
    Uniformly draw item $vj(vj \neq vi)$ from the time
    window of $u$ at time $t$
    $u' \leftarrow (1- )u+ (1-p(vi >utvj)) @ @u (ruvit-ruvjt)$
    $v'i \leftarrow (1- )vi+ (1-p(vi >utvj)) @ @vi (ruvit-ruvjt)$
    $v'j \leftarrow (1- )vj+ (1-p(vi >utvj)) @ @vj(ruvit-ruvjt)$
    $A'u \leftarrow (1 - )Au+ (1 - p(vi >utvj)) @ @Au (ruvit- ruvjt)$
    $u; vi; vj;Au \leftarrow u'; v'i; v'j ;A'u$
Until $L$ convergence
Return A;U;V.
```

3. RESULTS AND ANALYSIS

In our proposed system, the user can also search people lists for making as friend. This operation may provide only name of the people who are all register in this site. Then creating friend request with required interest lists then send to another person. Whenever another person authenticate, the person can additionally view all the friend request with system engendered interest value, this value represents the interest are matched between them. If another person may want to accept the friend request, otherwise, reject the requests. Whenever the profile picture is changed by the user, then the profile key is generated automatically. This profile key can be shared over the people, for view the profile by friends of every utilizer.

- ✓ Users Interests is consider for making friends request
- ✓ More Security for Profile information
- ✓

4. CONCLUSION:

We for the first time formalize the problem of privacy-preserving distributed profile matching in MSNs, and propose two concrete schemes that achieve increasing levels of user privacy preservation. Towards designing lightweight protocols, we utilize Shamir secret sharing as the main secure computation technique, while we propose supplemental enhancements to lower the proposed schemes' communication cost through extensive security analysis and simulation study. Predicated on the characterized gregarious behavioral profiles, we are able to distinguish the users from others, which can be facilely employed for compromised account detection.

REFERENCES:

[1] A. Ometov, K. Zhidanov, S. Bezzateev, R. Florea, S. Andreev, and Y. Koucheryavy, ‘‘Securing network-assisted direct communication: The case of unreliable cellular connectivity,’’ in Proc. IEEE 14th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom), vol. 1. Aug. 2015, pp. 826–833.

[2] Y. Najaflou, B. Jedari, F. Xia, L. T. Yang, and M. S. Obaidat, ‘‘Safety challenges and solutions in mobile social networks,’’ IEEE Syst. J., vol. 9, no. 3, pp. 834–854, Sep. 2013.

[3] HAOJIN ZHU1 (Member, IEEE), SUGUO DU2 , MUYUAN LI1 (Student Member, IEEE), AND ZHAOYU GAO1 (Student Member, IEEE),” Fairness-Aware and Privacy-Preserving Friend Matching Protocol in Mobile Social Networks”, revised 11 July 2013; accepted 15 July 2013. Date of publication 26 August 2013; date of current version 20 September 2013.

[4] S. Guha, K. Tang, and P. Francis, “Noyb: privacy in online social networks,” in Proceedings of ACM SIGCOMM Workshop on Online Social Networks. ACM New York, NY, USA, 2008, pp. 49–54.