Secure Profile Matching for Portable Public Networks

M. Ramanjulu
M. Tech (CSE)
MITS, Madanapalle
Chittoor, India

M. Veeresh Babu
M. Tech
Assistant Professor (CSE)
MITS, Madanapalle
Chittoor, India

ABSTRACT
In portable public networks creation of the new connection is important service. Where an existing client can discover related users bounded by objects nearness of him/her. In Portable public networks we can provide connection to the best profile matching users only.

In general all the peoples frequently fill the information for profile before login in any portable public network. In this paper the existing user can see all the profiles by using search option. Here the problem is the existing user can see the profiles of the unknown users and hack the information. In this paper we proposed the security to the user's profiles by using with malicious model. Here matching profiles will be display but non matching profiles will not display. The problem is even we search the known person profile that profile will not match to yours profile then we cannot see the profile. So to overcome the problem by sending a request to the known user, the user will accept the request then the profile will display.

General Terms
Profile matching**,** Security analysis, Malicious Model, Honest but Curious Model can be used to providing security.

Keywords
Bluetooth, Portable Public Networks, HBC, SMC.

1. INTRODUCTION
Social networking is where individuals with similar interests connect with each other through their mobile/tablet. They form virtual communities. For example face book, Twitter, LinkedIn etc. What makes public network sites single is not that they allow individuals to meet strangers, but rather that they enable users to fluent and build observable their public networks. On a lot of the big SNSs, participant are not automatically "networking" or looking to convene new group; as a substitute, they are mainly communicate with public who are by now a part of their total public network. To stress this spoken public network as a serious organizes mark of these sites, we label them "public network sites." [1]

However, such systems and lift an integer of isolation concerns. Let us first observe an inspiring situation. In a hospital, patients may contain their disease symptoms and medications in their own profiles in arrange to discover comparable patients, for material or normal maintain. In this situation, an initiating client (initiator) can feel like to discover away the patient having the most number of matching symptoms with her, though person unwilling to reveal her sensitive disease information to the rest of the users, and the equal for the user's person coordinated through users' individual profiles are directly exchanged among all other, it resolve construct simple client profiling anywhere that in order can be just collected by a close to customer, also in an dynamic or inactive way; and those user information may be broken in illegal ways. For example, a naresh as of a pharmacy can present denote parallel queries to get information on patients' medications for promotion purposes. To cope with user profiling in MSNs, it is essential to release least amount and crucial own in sequence to as few users as possible [4].

The existing mobile social network systems give small regard to the safety and solitude concerns related with helpful one's own social networking preferences and convenience in order to the everywhere computing location. In particular, in mobile social networks, the mobile users may face the risk of leaking of their personal information and their location privacy. Under this circumstance, the attackers can directly associate the personal profiles with real persons nearby and then launch more advanced attacks [3].

Normally talking, Private Set Intersection is a cryptographic protocol that involves two players, Raj and Dab, each with a private set. Their goal is to compute the intersection of their respective sets, such that minimal information is revealed in the process. In additional words, Raj and Dab must study the basics (if any) familiar to both sets and zero (or as little as possible) else. This can be a common procedure where, perfectly, neither party has any benefit over the other [7].

2. EXISTING SYSTEM
In the existing system the user before login the portable public networks create the profile with personal information. The each and every profile may have the sensitive information about user. Generally the login user search the other users enter the new user name. The new user information will display the new user is may know person or unknown person. The new user profile not having the security new user information will not having security [5].

We think plans speak throughout wireless interfaces such as Bluetooth or WIFI. For directness, we think every participating tool is in the memo collection with each other. In calculation, we think that a secure statement control has been conventional among each pair of users. We cannot guess the being of a trusted third party through the protocol run; all party take summary related in a entirely spread way. They may help with each other, i.e., when *P*1 runs the process with each *Pi*, a subset of the rest of parties would help them to estimate their cost. Note to, provided to incentives used for the users to help a crucial topic, and near several existing mechanisms [2].

A typical friend discovery process could be described as follows. User *A* will send his current interest I*A* to user *B*, and then he will obtain *B*'s current interest I*B*. After the interests are exchanged, *A* will compare his own profile P*A* with I*B* while *B* compares his profile P*B* with I*A*. We define a successful matching as P*A* matches I*B* and, at the same time, P*B* matches I*A*, which is similar to the privacy level introduced in. Note that, in some cases, the user only cares about some specific attributes. To deal with those fields that are not considered in one query, we separate the fields of I

into interested fields (IF) and non-interested fields (NIF). Therefore, a successful matching should ensure the IF fields of the interests and profiles match while whether NIF fields match or not cannot affect the final comparison results [6].

2.1 Disadvantages

- In existing system the user profile containing sensitive information that information will be seeing all the existing users.
- Lack of a security to the users profile information.
- Chance to attack the hackers to take information and doing other activities.
- The users profiles containing the risk doing online scams with profile information.
- Finally the users profile information will be lost the security and efficiency.

3. PROPOSED SYSTEM

In this paper, overcome the existing system problems and introduce the proposed system techniques. In existing system user profile not having security so we provide the security by using the novel protocol. After providing the security the matching users profiles information will display. The matching user can be identify based on same location directly display then location will be different it's not display directly. In proposed system the existing user can find new user the user name will be display and matching attributes will display but not display the unmatched attributes and we search known person profile that profile will not match to yours profile not display any information. This paper is mainly concentrate on the desires so we propose the matching profiles will display directly with location based and desires based and proposed to the request option to new users [2].

In this paper, we are mostly involved insiders, who are legal participators of the related procedure and try to achieve user profile, i.e., find as really own summary information of other near users as achievable. For example, with a user's attributes, a bad man can compare and recognize that user via its MAC addresses or community keys. Though, we cannot completely avoid user profile, because at least the maker and its best similar user will equally study their connection position. Thus we focus on minimize the amount of personal information exposed in one practice scamper. The main opposition representation measured in this paper is *honest-but-curious* (HBC), i.e., member motivations infer personal information from procedure but directly follow the protocol. while we do not specially deal with the malicious attacker model where an challenger may well inside chance from the protocol run, we will discuss how your protocols can be total to get security in that model. The challenger may take action alone or some parties may collude. This summary consists of multiple attributes (e.g., user's occupation, hobbies and other private information) [9].

Proposed system match the two users based on the distance between their social coordinates in an online social network. By using secure multi-party computation (SMC) techniques, it can achieves that, an initiating user can find from a group of users the one whose profile best matches with his/her. it proposed the concept of Fine-Grained Private Matching, which allows finer differentiation between users and can support a wide range of matching metrics at different privacy levels. Different from these existing works, we separate users' profiles from their interest for the first time. The proposed scheme could well thwart this novel attack and thus achieve a better security. The adversary is considered to be curious with others' profile and interest. Therefore, if without an appropriate security countermeasure, the friend discovery process may suffer from a series of privacy threats [10].

3.1 Advantages

- The proposed system used to providing security to the all user profiles and not access the information to the other users.
- The matching user's information will be display but not matching users information not display.
- We can see the users profile information we can send the request and take acceptance message after we can see the profile.
- Reduce the time to search the matching users why because the matching profiles will display directly.

4. IMPLIMENTATION

In paper, proximity-based customer finding and key group are two main issues for the usability of your outline parallel protocols. We make up to your FindU method can be used in moveable strategy set with partial wireless interfaces like Wi-Fi or Bluetooth (most of today's stylish phones have both interfaces), and create lively in the adhoc mode. We contain done a few previous work in helpful belief initialization in wireless networks. Here we explain possible setup processes that involve little person effort. User finding if using Bluetooth, the available Service Discovery Protocol (SDP) can be utilized near explore for close by FindU users. The SDP procedure can be worn to circulate/replace in sequence [1].

We can capable to use it to begin the protocol. For Wi-Fi, the ad-hoc mode would be adequate for device detection. Key institution as pair wise keys should be conventional between all nearby plans, a simple design would require $O(N2)$ density. To get key validity, we can believe tamper-evident pairing (TEP), in which any alter of key trade communication among two users by an aggressor will be detected. While TEP was implemented in the two-party situation, the identical plan container and exist helpful to broadcast. In this method, the message and time difficulty is only $O(N)$.In adding, it is fully spread and do not need any middle server. Really this approach is further helpful for Wi-Fi devices with better-off resources though, for Bluetooth devices it can also be worn [5].

4.1 Modules

4.1.1 Security

The user may contain dissimilar privacy levels we can provide the security to the profiles by using the two protocols PSI and PCSI. By using the two protocols providing security and efficiency to the profile information. In this security module we can provide privacy to the profiles easily. The security module the user's profiles having more secure comparing to other social network profiles [6].

4.1.2 Usability and Efficiency

The summary same in portable public networks, it is attractive to involve to users communication possible simply. In this project the client just wants to clearly contribute in the conclusion of the process run. The summary similar formation design should be lightweight and practical, i.e., being enough efficient in calculation and message to be used in MSN. Finally, the usability and capability module providing flexibility to the users profiles and their privacy levels [13].

4.1.3 Shamir Secret Sharing Scheme

The Shamir secret sharing scheme module is multi-party protocols related to key organization. The novel enthusiasm for secret sharing was the following. To protect cryptographic keys from loss, it is popular to create backup copies. The better the number of copies made, the better the risk of safety contact; the minor number, the larger risk that all are lost. This module will be addressing this issue by allowing improved consistency lacking bigger risk [12].

4.1.4 Preventing Malicious Attacks

Our protocols in this paper are only recognized secluded in the HBC model; it would be interesting to make it secluded in the stronger mean copy, i.e., to stop a rival from accidentally unlike from a training sprint. We showed that with an extra assure about prior to last rebuilding (which adds little extra slide), a complete kind of "set rise attack" can be just prohibited .where a mean user influences the last making in her positive way by varying his shares subsequent others [4]'.

5. ARCHITECTURE

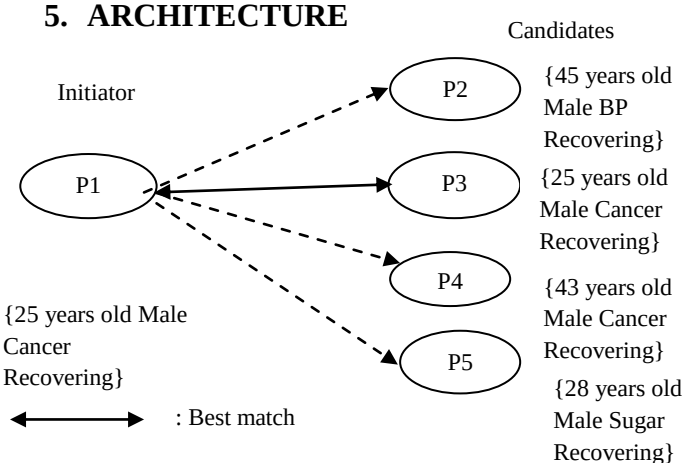

Fig 1: Best matching information will be display

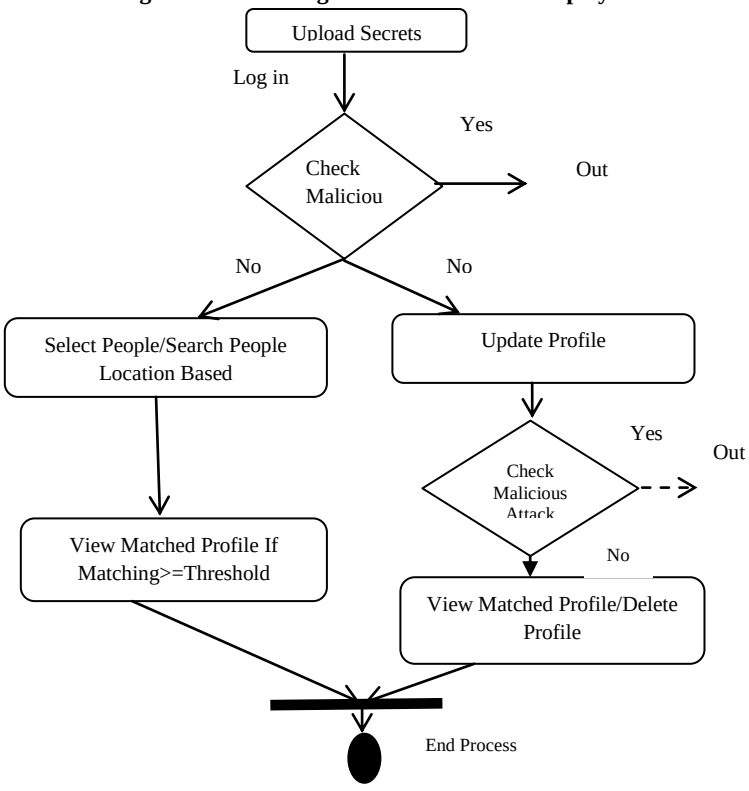

Fig 2: Architecture of profile matching

5.1 Algorithm

Without loss of the generality, we consider two nodes *Ua* and *Ub* for potential friend discovery [10]. In the system initialization phase, the trusted third party will generate their private and public key pairs, which are denoted as (*ska*, *pka*) and (*skb*, *pkb*), respectively. Their profiles are denoted as P*a* and P*b*. For a matching, *Ua* and *Ub* may Modulesonly consider *ea* and *eb* out of total *n* interest fields. We assume the current interest vectors are I*a* and I*b*.

Algorithm:

Step 1: Start

Step 2: Establish Connection

Step 3: Login if existing user or signup for new user

Step 4: Search Profile

a. Single Step KNN

b. Multi Step KNN

Step 5: If Profiles are matched view details of authorized user whose profile is matched

Step 6: Start Communication

Step 7: Stop

6. RESULTS

Table 1: Number of query attributes with protocol run time

Number of query attributes X-axis	**Total protocol runtime in (seconds) Y-axis**	
	Basic runtime	**Advance runtime**
0	**0**	**0**
10	**0.5**	**0.5**
20	**1**	**0.8**
30	**1.5**	**1**
40	**2**	**1**
50	**2.5**	**1**

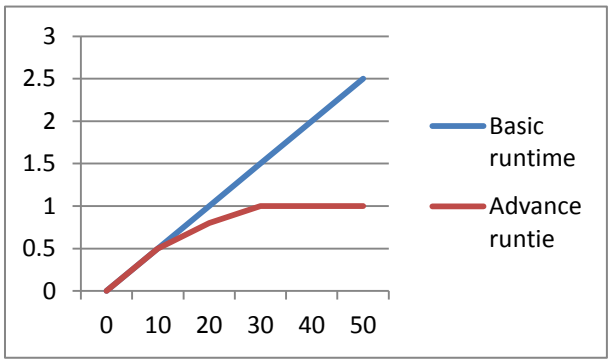

Fig 3: Total protocols run time

Table 2: Number of candidates attributes with energy consumption

Number of candidate attributes X-axis	Energy consumption in (joules) Y-axis	
	Basic Energy	Advance Energy
0	0	0
100	4	4
200	8	5
300	12	8
400	16	8
500	20	8

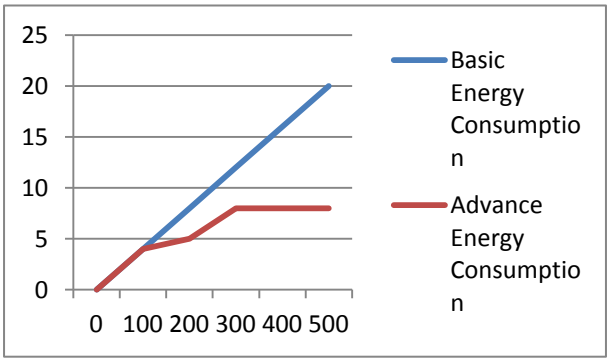

Fig 4: Energy consumption with number of customer attributes

7. CONCLUSION AND FUTURE ENHANCEMENT

7.1 Conclusion

In this paper, we can find out the problem in portable public networks is the lack of security problem to the user's profiles. We can provide security to profiles by proposing the malicious model. We use Shamir covert contribution as the main protected calculation system. During general protection study and recreation learn, we demonstrate that our schemes are recognized safe than the HBC model. We have developed a novel protocol that will ensure the fairness and the privacy of profile matching process in portable public networks [5].

7.2 Future Enhancement

This paper provides the security to the user's profiles fully but not providing good communication, here future enhancement is to provide good communication to the two users. This paper matches profiles based on the location selected. The profile matching information will be display only location based but not other information. Future extension is providing security with good efficiency and communication. While we suggest extra enhancements to minor planned schemes message costs

8. ACKNOWLEDGMENTS

I sincerely thank to MANAGEMENT of MADANAPALLE INSTITUTE OF TECHNOLOGY AND SCIENCE for providing excellent infrastructure and lab facilities that helped me to complete this paper.

9. REFERENCES

[1] Giles Hogben, ENISA (2007),ENISA Position Paper No.1 "Security Issues and Recommendations for Online Social Networks"

[2] Elie Raad, Richard Chbeir, and Albert Dipanda," User Profile Matching in Social Networks" in Byourgogne University Dijon, France.

[3] Ralph Gross and Alessandro Acquisti,"Information Revelation and Privacy in Online Social Networks"

[4] Rui Zhang _ , Yanchao Zhang _ , Jinyuan (Stella) Suny, and Guanhua Yanzn, "Fine-grainedPrivate Matching for Proximity-basedMobile Social Networking".

[5] Muyuan Li, Zhaoyu Gao, Suguo Du, Haojin Zhu, Mianxiong Dong, KaoruOta,"PriMatch: Fairness-aware Secure Friend Discovery Protocol in Mobile Social Network".

[6] Q. Ye, H. Wang, and J. Pieprzyk, "Distributed private matching and set perations," in *ISPEC'08*, 2008.

[7] E. D. Cristofaro and G. Tsudik, "Practical private set intersection protocols with linear complexity," in *Financial Cryptography and Data Security '10*, 2010.

[8] L. Kissner and D. Song, "Privacy-preserving set operations," in *CRYPTO '05, LNCS*. Springer, 2005.

[9] A. C. Yao, "Protocols for secure computations," in *SFCS82*,1982.

[10] D. Dachman-Soled, T. Malkin, M. Raykova, and M. Yung, "Efficient robust private set intersection," in *ACNS '09*, 2009.

[11] G. S. Narayanan, T. Aishwarya, A. Agrawal, A. Patra, A. Choudhary, and C. P. Rangan, "Multi party distributed private matching, set disjointness and cardinality of set intersection with information theoretic security," in *CANS '09*. Springer - Verlag, Dec. 2009.

[12] C. Hazay and Y. Lindell, "Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries," in *TCC'08*, 2008.

[13] S. Jarecki and X. Liu, "Efficient oblivious pseudorandom function with applications to adaptive ot and secure computation of set intersection," in *TCC '09*. Berlin, Heidelberg: Springer-Verlag, 2009.

[14] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in *IEEE INFOCOM '11*,Apr 2011.

[15] E. De Cristofaro, M. Manulis, and B. Poettering, "Private discovery of common social contacts," in *Applied Cryptography and Network Security*, Springer, 2011.