PROFILE MATCHING OF SECURED/PROTECTED MULTI-PARTY COMPUTATION

K. Praveen Kumar Goud[1], J. Pradeep Kumar[2]
[1]M.Tech, CSE Dept, MLRIT, Hyderabad
[2]M.Tech(IT), Asst. Professor, MLRIT, Hyderabad

***Abstract*— The Profile identical means two users comparing their individual profile and is frequently the first step towards effectual PMSN. It, however, conflicts with the users' growing isolation concerns about disclosing their individual profiles to complete strangers before deciding to relate with them Our protocols make possible two users to carry out outline similar without disclosing any data about their accounts/profiles ahead of the judgment result. Making new associations according to personal preference is a essential service in mobile social networking, where an initiate user can find matching users within physical propinquity of him/her. In an existing systems for those services, frequently all the clients directly publish their full profiles for remaining of them to search. Though, in much submission, the users' personal outline may contain sensitive in order that those do not want to create it open thing. In this paper, we explored a set of privacy-preserving profile identical themes for mobile social networks which are based on proximity. In an initiate client can discover from a set of clients the one whose profile/account greatest counterpart with her / his; to restrict the danger of secure disclosure, only required and least information about the confidential characteristic of the partake users is exchanged. Two the increasing levels of user solitude are distinct, with falling amounts of exposed profile/account data. Leveraging secured/protected multi-party computation (SMC) method we propose novel modus operandi that understand each of the client privacy levels, which can also be adapted by the users. We bring in formal security proofs and presentation evaluation on our system, and show their compensation in both security and good organization over state-of-the-art methods. The social familiarity between two clients/users as the identical metric, which can measure the distance between their social coordinate with each being a vector pre calculated by a central server which is trusted to stand for the location of a client in an online social network. By judgment, our work does not rely on the link of PMSN clients with a one social network in online and talk to a more general classified identical crisis for PMSN by helping fine-grained private profiles/account and a huge spectrum of corresponding metrics.**

I. INTRODUCTION

With the propagation of mobile devices, mobile social networks (MSNs) are becoming an indissoluble part of our lives. Leveraging set of connections portable devices such as smart phones and PDAs as platforms, MSN not only enables people to use their accessible online social networks (OSNs) at anywhere and anytime, but also set up a countless of mobility-oriented use such as location-based services and increased reality. Among them, an important service is to make new social associations/associates within physical proximity based on the matching of individual profiles. For example, MagnetU and E-SmallTalker [2] are MSN appliance that match one with nearby people for dating or friend-making based on common interests. In such an appliance, a user only needs to input some characteristic in her profile, and the scheme would be mechanically find the persons around with similar sketch The scopes of these submission are very broad, since people can put input anything as they want, such as hobbies, phone contacts and places they have been to. The final can even be used to find hhh"lost connections" and "familiar strangers". However, such systems also raise a number of privacy concerns. Let us first examine a motivating scenario. In a hospital, patients may include their illness symptoms and medications in their personal profiles in order to find similar patients, for physical or mental support. In this scenario, an initiating user (initiator) may want to find out the patient having the maximum number of identical symptoms with her, while being unwilling to disclose her receptive illness information to the rest of the users, and the same for the users being coordinated with. If users' private outline are directly swap with each other, it will help user profiling where those in order can be easily unruffled by a nearby user, either in an active or passive way; and those user in sequence may be exploited in illegal ways. For example, a salesman from a pharmacy may submit hateful identical doubt to obtain statistics on patients' prescription for marketing purposes. To cope with user outline in MSNs, it is necessary to disclose minimal and essential personal information to as few users as probable. In fact, the ideal situation is to let the initiator and its best matching user directly and privately find out and connect to each other, without knowing anything about other users' profile attributes, while the rest of the users should also learn nothing about the two user's matching attributes. However, it is challenging to find out the matching users privately while efficiently. One may think of simply turning off the cell phone or input very few attributes, but these would interfere with the system usability. Recently, Yang et. al. proposed E-SmallTalker [2], a practical system for matching people's interests before initiating a small-talk. However, E-SmallTalker suffers from the dictionary attack which does not fully protect the non-match attributes between two users. Another difficulty of private matching under a MSN setting is the lack of a centralized authority. Lu et. al. [3] future indication of an identical schemes for mobile health social networks, arrogant the existence of a semi-online central power.

In this paper, we trounce the above test and make the following main support

(1) We invent the solitude continuation of profile matching problem in Mobile Social Network. Two levels of isolation are defined along with their hazard models, where the higher time alone level leaks less profile in sequence to the opponent than the subordinate level.

(2) We advise two fully circulated privacy-preserving profiles like schemes, first one is a PSI (private set connection) protocol and the next one is a PCSI (private cardinality of set-intersection) protocol. However, answers based on existing private set connection schemes are distant from capable. We manipulate secure multi-party computation (SMC) based on polynomial confidential sharing, and offer a lot key development to improve the calculation and message efficiency. Also users can choose modified privacy levels when running the same matching instance.

(3) We provide formal security proofs and extensive performance evaluation for our schemes. Our two protocols are shown to be secure under the honest-but-curious (HBC) model, with information-theoretic security (for PSI) and standard security (for PCSI), respectively. We also discuss possible extensions to prevent malicious attacks. Meanwhile, they are shown to be more efficient than previous schemes that achieve similar security guarantees under the typical settings of MSN.

II. PROBLEM STATEMENT

Existing System: In existing organization for those services, generally all the clients openly print their complete outline for others to search. However, in many request the clients' private profiles may include sensitive data that they don't desire to create community.

Disadvantage:-

Opens up the opportunity for hackers to commit deception and begins spam and attack of virus will get started. It gradually increases the danger of clients declining prey to online cheat that seem authentic, resulting in data or individuality stealing.

May result in unhelpful commentary from employees about the company or possible legal penalty if employees use these sites to view offensive, illicit or disgusting material. Potentially results in lost output, particularly if employees are busy in updating profiles.

Proposed System: In this thesis, we rise above the test and make the following main charity.

(1) We create the confidentiality safeguarding the trouble of profile identical in mobile social network. Couples of levels of confidentiality are described in addition with their threat replicas where the top confidentiality level leaks less profile in sequence to the opposition than the lower level.

(2) We put forward two fully distributed privacy-preserving report matching schemes, first one of them is a personal set meeting point protocol and next one is a personal cardinality of group-intersection protocol. Though, explanations depended upon previous private set connection schemes are distant from proficient. We influence protected multi-party adding up based on polynomial secret spreading, and suggest a lot key growth to improve the calculation and communication effectiveness.

Pros:-

PMSN (Proximity-based mobile social network) becomes more and more popular due to the unstable growth of smart phones.

Two equally distrust parties, each holding a confidential data set, jointly calculate the junction or the connection cardinality of the couple of sets without seep out any additional in sequence to either party make easy open communication, leading to improved in order discovery and delivery. Allows employees to talk about the new ideas, post news, ask query and share links. Provides an chance to widen business contacts. Targets wide viewers, making it a useful and effective employment tool. Improves business standing and client base with least use of publicity. Expands marketplace research, implements marketing campaigns, delivers infrastructure and directs attracted people to specific web sites.

III. SYSTEM DEVELOPMENT

- Protection
- Usage and effectiveness
- Shamir private sharing scheme
- Blocking Malicious Attacks

Protection: Since the users may have dissimilar isolation rations and it acquires variant amount of hard work to accomplish them, we hereby describe couple levels of confidentiality where the privileged level leaks less in rank to the foe.

Usage and effectiveness: For report toning in MSN, it is popular to involve as few human relationships as probable. In this thesis, a human user only need to plainly participate in the end of the set of rules run, e.g., decides whom to tie to base on the universal interests. In accumulation, the makeup design should be lightweight and realistic, i.e., being sufficient efficient in addition and communication to be utilized in mobile social networking. At last, various clients/customers (Particularly the candidates) shall have the alternative to personalize their confidentiality levels flexibly.

Shamir private sharing scheme: Top secret sharing schemes are multi-party protocol related to key business. The original enthusiasm for top secret distribution was the following. From loss to preserve cryptographic keys, it is pleasing to generate backup replicas. The superior the figure of duplicate made the better the risk of security contact; the smaller the figure, the better the risk that all are lost. Secret allocation schemes address this issue by allowing better trustworthiness without better risk.

Malicious Attacks Blocking: In this paper our protocols are only proven protected in the HBC model; it would be attractive to create it protected under the effective malicious replica that means to verify an opponent from at random conflicting from a protocol function. we explored that with an additional promise round before final rebuilding (which inserts few additional further), a detailed type of “set increase attack” can be easily disallowed where a malicious user pressure the ultimate output in her positive way by altering her divides after watching others.

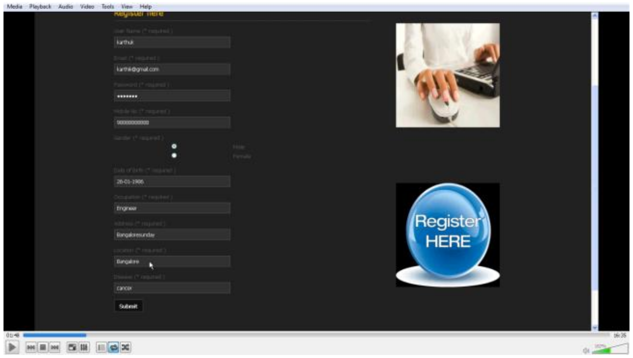
IV. RELATED WORK

PMSN (Proximity-based mobile social networking) refers to the social communication among bodily proximate mobile users directly through the Bluetooth/Wi-Fi interface on their smartphones or other mobile devices. It becomes more and more popular due to the recently unstable growth of smartphone users. Profile corresponding means two users contrast their individual profiles and is often the first step towards effectual PMSN. It, however, conflicts with users’ growing privacy concerns about reveal their personal profiles to complete strangers before decide to interact with them. This paper tackles this open challenge by conniving a suite of novel fine-grained private matching protocols. Our protocols facilitate two users to perform profile matching without disclosing any in sequence about their profiles beyond the assessment result. In contrast to existing coarse-grained private identical schemes for PMSN, our procedure allow finer separation between PMSN users and can support a wide range of matching metrics at unlike privacy levels. The security and communication/computation overhead of our protocols are thoroughly analyzed and evaluated via detailed imitation Proximity-based mobile social networking (PMSN) be- comes more and more accepted due to the volatile growth of smartphones. In particular, eMarketer estimated the US and worldwide smartphone users to be 73.3 million and 571.1million in 2011, respectively, and almost all smartphones have Wi-Fi and Bluetooth interfaces. PMSN refers to the collective communication in the middle of physically nearby mobile users in a straight line from side to side the Bluetooth/Wi-Fi interfaces on their smartphones or other mobile devices. As a valuable balance to web- based online social networking, PMSN enables more touchable face-to-face social connections in public places such as bars, airports, trains, and stadiums [1]. PMSN is conducted via applications running on smart- phones or other mobile devices. Such applications can be offered by small independent developers. For instance, there are currently over 50 Bluetooth/Wi-Fi chatting applications in the Android Market for Android devices and 60 in the App Store for Apple devices. Developing advanced Bluetooth/Wi-Fi social networking applications also has recently attracted attention from the academia [1]. Moreover, online social network providers such as Facebook and Twitter may add PMSN functionalities to their future applications for smartphones and other mobile devices.

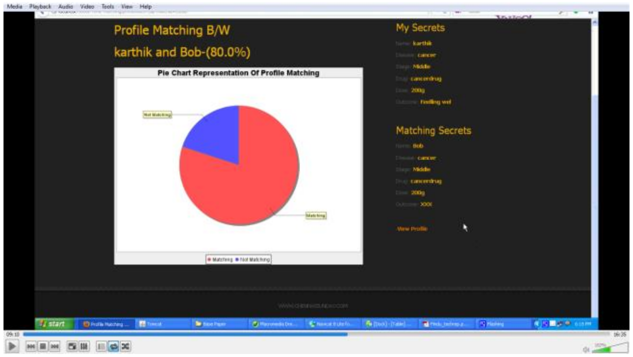
Private (profile) matching is indispensable for fostering the wide use of PMSN. On the one hand, people normally prefer to socialize with others having similar interests or background over complete strangers. Such social reality makes profile matching [2] the first step towards effective

PMSN, which refers to two users comparing their personal profiles before real interaction. On the other hand, people have growing privacy concerns for disclosing personal profiles to arbitrary persons in physical proximity before deciding to interact with them [2]–[5]. Although similar privacy concerns also exist in online social networking, preserving users' profile privacy is more urgent in PMSN, as attackers can directly associate obtained personal profiles with real persons nearby and then launch more targeted attacks. This situation leads to a circular dependency between personal-profile exchange and engagement in PMSN and thus necessitates private matching, in which two users to evaluate their special profiles without reveal them to each other.

V. RESULTS



User Name (* required)
karthuk
Email (* required)
karthik@gmail.com
Password (* required)
••••••••
Mobile No (* required)
9000000000
Gender (* required)
○ Male
● Female
Date of Birth (* required)
28-01-1986
Occupation (* required)
Engineer
Address (* required)
Bangaloresunday
Location (* required)
Bangalore
Disease (* required)
cancer



Media Playback Audio Video Tools View Help

Profile Matching B/W karthik and Bob-(80.0%)

Pie Chart Representation Of Profile Matching
Not Matching
Matching
● Matching ● Not Matching

My Secrets
Name: karthik
Disease: cancer
Stage: Middle
Drug: cancerdrug
Dose: 200g
Outcome: Feeling wel

Matching Secrets
Name: Bob
Disease: cancer
Stage: Middle
Drug: cancerdrug
Dose: 200g
Outcome: XXX

View Profile
start
09:10
06:35

VI. CONCLUSION

In this thesis, we for the earliest occasion observe the problem of privacy-preserving dispersed profile identical in MSNs, and suggest two real system that attain growing levels of user time alone conservation. Towards designing lightweight protocols, we make use of Shamir secret sharing as the main secure working out technique, while we suggest additional enhancement to inferior the future schemes' message expenses. Through broad security analysis and model study, we show that 1) our format are known protected beneath the HBC model, and can be simply general to thwart sure lively attacks; 2) our schemes are much more well-organized than state-of the- art ones in MSNs where the system size is in the tens order, and when the quantity of inquiry attribute is slighter than the number of information attributes.

REFERENCES

[1] M. Li, N. Cao, S. Yu, and W. Lou, "Findu: Privacy-preserving personal profile matching in mobile social networks," in IEEE INFOCOM '11, Apr 2011, pp. 1–9.

[2] Z. Yang, B. Zhang, J. Dai, A. Champion, D. Xuan, and D. Li, "Esmalltalker: A distributed mobile system for social networking in physical proximity," in IEEE ICDCS '10, June. 2010. 11

[3] R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for mhealthcare social network," Mobile Networks and Applications, pp. 1–12, 2010.

[4] C. Zhang, X. Zhu, Y. Song, and Y. Fang, "C4: A new paradigm for providing incentives in multi-hop wireless networks," in INFOCOM, 2011 Proceedings IEEE, april 2011, pp. 918 –926.

[5] M. Freedman, K. Nissim, and B. Pinkas, "Efficient private matching and set intersection," in EUROCRYPT'04. Springer- Verlag, 2004, pp. 1–19.

[6] Q. Ye, H. Wang, and J. Pieprzyk, "Distributed private matching and set operations," in ISPEC'08, 2008, pp. 347–360.

[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, pp. 241–257.

[9] A. C. Yao, "Protocols for secure computations," in SFCS '82, 1982, pp. 160–164.

[10] D. Dachman-Soled, T. Malkin, M. Raykova, and M. Yung, "Efficient robust private set intersection," in ACNS '09, 2009, pp. 125–142.

[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, pp. 21–40.

[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, pp. 155–175.

First Author: ***K. Praveen Kumar Goud*** received B.Tech from Geetanjali Institute of Science and Technology, Hyderabad, in the year 2012. He is currently M.Tech student in Computer Science and Engineering Department from MLR Institute of Technology. And his research interested areas are in the field of Cloud Computing, Mobile Computing, Networking and Information Security.

Second Author: J Pradeep Kumar working as an Asst. Professor in MLR Institute of Technology, Dundigal, Ranga Reddy. He has completed his M.Tech CSE and he has 2 years of teaching experience. His research interested areas are DBMS and Software Engineering.

Third Author: G Kiran Kumar is working as Associate Professor & HOD-CSE in MLR Institute of technology. He did M.Tech from Osmania University, Hyderabad, and submitted Ph.D from Nagarjuna University. His research areas include Data Mining, Spatial data mining, Software Engineering.