Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 6, June 2014, pg.958 – 963

RESEARCH ARTICLE

Analysis of Mobile Social Networking & Emergence of Proximity Based Mobile

[1]Dr. Nagu Chandra Shekhar Reddy, [2]G.Ramanujan

[1]Professor, Dept. of CSE, Institute of Aeronautical Engineering, India

[2]PG Scholar, Dept. of CSE, Institute of Aeronautical Engineering, India

Abstract – Mobile social network is essentially relational rather than attribute based on the unit analysis the individual but structures that consist of at least two social entities and the links among them. Search a friend in mobile social network profile matching two users comparing their personal profiles and conflicts with users growing privacy concerns about disclosing the personal profile to complete strangers before deciding to communicate with them. To perform profile matching without disclosing any information about their profiles beyond is a crucial in mobile social networking where the user can match with profile details of the request user. Existing service all the users directly publish their complete profiles for other to search it may contain sensitive information we analyze FindYou is solution of privacy preserving profile matching schemes for proximity based mobile networks from group of profiles that best matches to limit. This paper compare early search user profile process and the proposed one risk of privacy exposure only necessary information, FindYou is only search whether profile matches with the friend request hidden all other information.

Keywords - Privacy, Mobile Social Networks, Professional Profiles, PBMSN, Authorization

I. INTRODUCTION

Social networking is built on the idea is determinable structure to know each other direct or indirect personal relationships have popularized the idea that people can be connected through common associates. Idea from social networking to drive innovative design focus to close our own intellectual home design development and study of social technologies at the level of individuals groups and organizations although refer to the broader issue of business community and societal impact.

Mobile devices social networks is an inseparable part of our day activities networked portable devices such as smart phones an chips as a platform of mobile social networks not only

© 2014, IJCSMC All Rights Reserved

one person useful for each and every person to communicate like online social networks at anywhere at time mobile oriented applications such as location based services and augmented. Important service is to make social connections colleague with in physical proximity based on the matching of personal profiles. Early we have option of MagnetU and SmallTalker are mobile social networks that only nearby people for communication based on interest such an application user only needs to input query attributes in there profile and the system would automatically find the persons around with similar profiles. These application scopes are very broad, since the user can input anything as they want, such as hobbies, phone contacts and places they have been to. The latter can even be used to find lost connections and familiar strangers 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 reluctant to disclose her sensitive illness information to the rest of the users, and the same for the users being matched with. If users' private profiles are directly exchanged with each other, it will facilitate user profiling where that information can be easily collected by a nearby user, either in an active or passive way; and that user information may be exploited in unauthorized ways. For example, a salesman from a pharmacy may submit malicious matching queries to obtain statistics on patients' medications for marketing purposes. To cope with user profiling in MSNs, it is essential to disclose minimal and necessary personal information to as few users as possible.

II. Survey on Privacy Preserving Social Networks

The fundamental relation in a social networks between two members of the network carries the understanding of communication from the offline world, the formal establishment of a communication relation in a social network is only the matter of a mouse click preceding activities for agreeing to engage in communication resemble the offline world. Social network conveys the ability to perform privileged operations such as reading private content friend may see more details of know friend profile that an ordinary user. Friends may meet long time after if the symmetry of friendship relation matches the strongly in nature of self-disclosure and sustains the reciprocity of the data disclosure.

Assume the protection of the user's privacy to be the main objective for social networks not only encompass the protection of personal information which users publish at their profiles. The details of messages have to be hidden so only the requesting and responding parties should know one another identity and the content of the request finally disclosure of information about a third party to some member that is not explicitly trusted by the third party without the consent of the latter has to be prevented. Requiring explicit disclosure directly leads to the need for access control to information on a user may only be granted by the user directly and the access control has to be as fine grained as the profile and each attribute has to be separately manageable. User's identity and data must be protected against unauthorized modification detection and message authentication integrity in the context of online social network has to be extended parties in an online social network are arbitrary devices but real unambiguously identifiable persons.

© 2014, IJCSMC All Rights Reserved

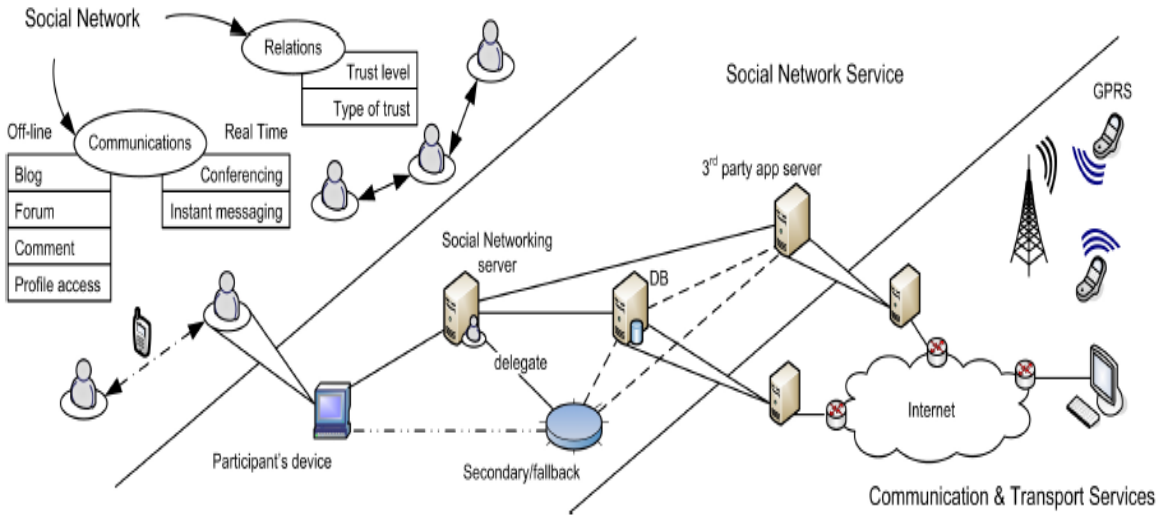

Figure 1 shows the Social Network Communication between professional users

Creation of person bogus accounts cloned accounts or other types of impersonation social network is easy to achieve user have strong inherent trust in online social networks and it has been shown that this combination may lead to a new kind of vulnerabilities. Consequence authentication has to assure the existence of real persons behind registered online social networks members identity checks do not necessarily have to be performed by a centralized service however all identification services have to be trusted by all users of social networks. Social network used as professional tools to aid their members business or careers data published by the users has to be continuously available user profiles in consequence is required as a basic feature even though considering recreational use the availability of some content may not seem a stringent requirement.

III. System Analysis on Privacy Preserving Mobile Social Network

Since the users may have different privacy requirements and it takes different amount of efforts to achieve to define two levels of privacy where the higher level leaks less information to the adversaries. For profile matching in MSN, it is desirable to involve as few human interactions as possible. In this paper, a human user only need to explicitly participate in the end of the protocol run, e.g., decide whom to connect on the common interests. In addition, the system design should be lightweight and practical, i.e., being enough efficient in computation and communication to be used in MSN. Finally, different users (especially the candidates) shall have the option to flexibly personalize their privacy levels. Secret sharing schemes are multi-party protocols related to key establishment. The original motivation for secret sharing was the following. To safeguard cryptographic keys from loss, it is desirable to create backup copies. The greater the number of copies made, the greater the risk of security exposure; the smaller the number, the greater the risk that all are lost. Secret sharing schemes address this issue by allowing enhanced reliability without increased risk. Our protocols in this paper are only proven secure in the HBC model; it would be interesting to make it secure under the stronger malicious model, i.e., to prevent an adversary from arbitrarily deviating from a protocol run. we showed that with an additional commitment round before final reconstruction (which adds little additional overhead), a specific type of

© 2014, IJCSMC All Rights Reserved

"set inflation attack" can be easily prevented where a malicious user influences the final output in her favourable way by changing her shares after seeing others'.

3.2. Proximity Based Mobile Social Networking: Assume that each user carries a mobile device with the internet packages and apps installed. The PSMN application can be developed by small independent developers offered by online social network service providers like Orkut Facebook Watsup as function module of their application built for mobile devices. More advanced PMSN applications have also been developed by the academia not differentiate a user from his mobile device involves two user and consists of three parts one is two users need discover each other in the neighbor discovery second is need to compare their personal profiles in the matching and other is two matching users enter the interaction for real information exchange. PMSN profiles matching the application developer defines a public attribute set consisting of d attributes $\{A_{1,\ldots} A_d\}$ where d is may range from several tens to several hundred depending on specific PSMN application attributes may have different meaning in different contexts.

IV. Problem Definition

Social networking platforms may allow organizations to improve communication and productivity by disseminating information among different groups of employees in a more efficient when it is not meant to be all inclusive the list below outlines some of the possible benefits. Provides open communication leading to enhanced information discovery and delivery allows employees to discuss ideas post news as questions and share links provides an opportunity to widen business contacts. Also improves the business reputation and client base with minimal use of delivers communications and directs interested people to specific web sites. At the same time opens up the possibility for hackers to commit fraud and launch spam virus attacks increases the risk of people falling prey to online scams that seem genuine resulting in data or identity theft. Potentially results in negative comments from employees about the company or potential legal consequences if employees use these sites to view objectionable illicit or offensive material. The golden rule of social networking is to avoid putting anything online that could reflect badly on our business acting unprofessionally could harm chances of getting a job or make poor impression on a new client. Even if we create social media for personal as well as professional networking we created with our nicknames to keep our account clean but the particular person may not contact if does not know the nick name to avoid all these issues we design a network privacy preserving distributed network.

V. Comparative Study

In existing systems for such services, usually all the users directly publish their complete profiles for others to search. However, in many applications, the users' personal profiles may contain sensitive information that they do not want to make public.Opens up the possibility for hackers to commit fraud and launch spam and virus attacks. Increases the risk of people falling prey to online scams that seem genuine, resulting in data or identity theft, the may result in negative comments from employees about the company or potential legal consequences if employees use these sites to view objectionable, illicit or offensive material and Potentially results in lost productivity, especially if employees are busy updating profiles compare to early system our work overcome the above challenges and contributions.

© 2014, IJCSMC All Rights Reserved

Formulate the privacy preservation problem of profile matching in MSN. Two levels of privacy are defined along with their threat models, where the higher privacy level leaks less profile information to the adversary than the lower level and propose two fully distributed privacy-preserving profile matching schemes, one of them being a private set intersection protocol and the other is a private cardinality of set-intersection protocol. However, solutions based on existing PSI schemes are far from efficient. We leverage secure multi-party computation based on polynomial secret sharing, and propose several key enhancements to improve the computation and communication efficiency pproximity-based mobile social networking (PMSN) becomes increasingly popular due to the explosive growth of smart phones.

VI. CONCLUSION

In this paper presents search tool such as FindYou for searching professional profile in social network group or an organization to find out some information which is needed. The specific approach of tool is characterized, it hidden the information which unwanted a technique that implements and can be used in mobile social networking to develop end products. Our work compares early online social networks with mobile social network in real time application to achieve a high rate of accuracy in the case storage in human understandable improve the efficiency and effort of developers.

References

[1] J. Scott, *Social Network Analysis: A Handbook*, 2nd ed., Sage Publications, 1991. M. Granovetter, "The Strength of Weak Ties," *Am. J. Sociology*, vol. 78, no. 6, May 1973, pp. 1360–1380.

[2] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks," in 18th Intl. World Wide Web Conference (WWW'09), 2009.

[3] "Modelling The Real Market Value of Social Networks," http://www.techcrunch.com/2008/06/23/modeling-the-real-marketvalue-of-social-networks/, 2008

[4] Z. Yang, B. Zhang, J. Dai, A. Champion, D. Xuan, and D. Li, "ESmallTalker: Genoa, Italy, June 2010, pp. 468–477.

[5] M. Li, N. Cao, S. Yu, and W. Lou, "FindU: Privacy-preserving personal profile matching in mobile social networks," in *INFOCOM'11*, Shanghai, China, Apr. 2011.

[6] M. Arb, M. Bader, M. Kuhn, and R. Wattenhofer, "VENETA: Serverless friend-of-friend detection in mobile social networking," in *WIMOB'08*, Avignon, France, Oct. 2008, pp. 184–189.

© 2014, IJCSMC All Rights Reserved

Authors:-

Dr. Nagu Chandra Shekhar Reddy, Professor, Dept. of CSE, Institute of Aeronautical Engineering, India

G. Ramanujan, PG Scholar, Dept. of CSE, Institute of Aeronautical Engineering, India. His research areas include Networking, Wireless Networks & Security.

© 2014, IJCSMC All Rights Reserved