Application of Health Care Social Network's - A Brief Review

PUSHPALATHA M[#1] and Dr. ANTONY SELVADOSS THANAMANI[*2]

[#] *Assistant Professor of Computer Science Maharani's Science College of Women, Mysuru, India*

[*] *Associate Professor & HOD, Research Department of Computer Science, NGM College, Pollachi, India*

***Abstract*— The growing HealthCare Social network's has adopted about the risks of online data sharing platforms to pose a privacy and security of personal data. The aim of this study is to identify the policy implications of using HealthCare Social network's and how stakeholders elaborate upon the privacy of health data. It helps the connections between two person's matched profiles. Users fulfill some criteria and matches user's profiles with nearby persons of common interest.**

***Index Terms*— HealthCare Social network's, Profile matching, Service Discovery Protocol, private set intersection**

I. Introduction

HealthCare Social Network's are virtual communities where users connect with each other around common problems and share relevant health data and have been increasingly adopted successful of medical professionals and patients. The growing use of HEALTHCARE SOCIAL NETWORK'S has prompted public concern about the risks such that online data-sharing platforms pose to the privacy and security of personal health data. This work implies a set of privacy risk introduced by social networking in health care.

Many proximity-based social networks are developed to facilitate connections between any two people, and also to help a user to find people with a matched profile within a certain distance.

Health Care Network's enable patients to share details of their medical conditions with people, who have the same or similar conditions the compare and contrast different diagnoses and treatments anywhere in the world. Patients can ask for advice and learn from each other, discuss test results. They compare how different medications or treatments and combinations of drugs might or might not be working.

For example let us consider a real world scenario where in a hospital, the patients may include their illness symptoms and medications in their personal profiles in order to find similar patients, so that the patients may get some physical and mental support for their illness.

The scenario is illustrated in Fig. 1.1, where the party P1 is the initiator and the others are called "candidates". P1's best matching user is P3, who shares the maximum number of symptoms with her. Since directly publishing all the profile attributes is undesirable, it is a challenging task to find out the matching users privately.

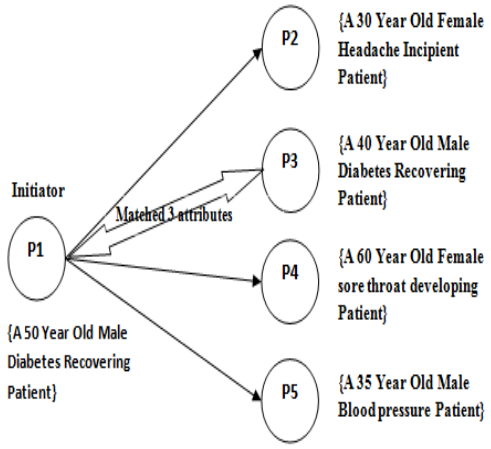
P2
{A 30 Year Old Female Headache Incipient Patient}
P3
{A 40 Year Old Male Diabetes Recovering Patient}
Initiator
Matched 3 attributes
P1
P4
{A 60 Year Old Female sore throat developing Patient}
{A 50 Year Old Male Diabetes Recovering Patient}
P5
{A 35 Year Old Male Blood pressure Patient}

Fig.1.1: Patient profile matching in healthcare social networks.

Unfortunately, in the above described scenario conflicts occur in matchmaking approach from a privacy point of view. Because an initiating user who wants to find out the matching patient having the maximum number of identical symptoms may broadcasts his/her sensitive illness information to the rest of the nearby users within his/her proximity. Here if the users' private profiles are directly exchanged with each other.

A. Motivation

Users are sharing incredible amounts of health data on social networking sites, although few of these sites offer either scientific accuracy or data protection. Considering the sensitivity of health data, people may not wish for their data to be revealed to unauthorized individuals and entities because such disclosure may negatively affect reputation, relationships and job opportunities.

II. Literature Review

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

This paper addresses the problem of maintaining the information privacy of user profiles that are being exchanged in a mobile social network. Making new connections according to personal preferences it forms a crucial service in mobile social networking, where the initiating user can find matching users within physical proximity of him/her. 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 disclose. This paper proposes the first privacy-preserving personal profile matching schemes called FindU for mobile social networks.

[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 June 2010.

Face-to-face interaction plays a big role in today's daily lives, especially for social networking purposes. Compared to other forms of social interaction that are separated by time and space boundaries, face-to-face interaction in physical proximity facilitates non-verbal communication. All people are not equally skillful in harnessing what physical proximity can offer to its fullest extent. A well-known barrier is the so-called social gap.

Small talk is a widely-used technique for shortening the social gap by initiating conversations about readily observable topics such as the weather. However, the effectiveness of small talk is limited if it only covers superficial weather-like topics.

E-SmallTalker automatically discovers and suggests topics such as common interests for more significant conversations. The work builds a Bluetooth Service Discovery Protocol (SDP) to exchange potential topics by customizing service attributes to publish nonservice- related information without establishing a connection also it proposes a novel iterative Bloom filter (IBF) protocol that encodes topics to fit in SDP attributes and achieves a low false positive rate.

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

Increasing dependence on anytime-anywhere availability of data and increasing fear of losing privacy motivate the need for privacy-preserving techniques. One interesting and common problem occurs when two parties need to privately compute an intersection of their respective sets of data. In doing so, one or both parties must obtain the intersection (if one exists), while neither should learn anything about other set. Although prior work has yielded a number of effective and elegant Private Set Intersection (PSI) techniques, the quest for efficiency is still underway.

This paper explores some PSI variations and constructs several secure protocols that are appreciably more efficient than the state-of-the-art. In today's increasingly electronic world, privacy is an important and precious commodity.

[4] Lan Zhang, Xiang-Yang Li, Yunhao Liu "Message in a Sealed Bottle: Privacy Preserving Friending in Social Networks" in IEEE ICDCS 2013

Many proximity-based mobile social networks are developed to facilitate connections between any two people, or to help a user to find people with a matched profile within a certain distance. A challenging task in these applications is to protect the privacy of the participants' profiles and personal interests. This paper focuses on designing of novel mechanisms, when given a preference-profile submitted by a user that searches persons with matching-profile in decentralized multi-hop mobile social networks. The mechanisms also establish a secure communication channel between the initiator and matching users at the time when the matching user is found. The rigorous analysis shows that the mechanism used is privacy-preserving (no participants' profile and the submitted preference-profile are exposed), verifiable (both the initiator and the unmatched user cannot cheat each other to pretend to be matched), and efficient in both communication and computation. Extensive evaluations using real social network data and actual system implementation on smart phones show that the mechanisms designed are significantly more efficient than existing solutions.

[5] Qi Xie and Urs Hengartner "Privacy-Preserving Matchmaking For Mobile Social Networking Secure Against Malicious Users" in IEEE 2011

The success of online social networking and of mobile phone services has resulted in increased attention to mobile social networking. Matchmaking is a key component of mobile social networking. It notifies users of nearby people who fulfill some criteria, such as having shared interests, and who are therefore good candidates for being added to a user's social network.

Unfortunately, the existing matchmaking approaches are troublesome from a privacy point of view. One approach has users' smart phones broadcast their owners' personal information to nearby devices. This approach reveals more personal information than necessary. The other approach requires a trusted server that participates in each matchmaking operation.

This paper proposes a privacy-preserving matchmaking protocol for mobile social networking that lets a potentially malicious user learn only the interests (or some other traits) that he has in common with a nearby user, but no other interests. In addition, the protocol is distributed and does not require a trusted server that can track users or that needs to be involved in each matchmaking operation. The paper presents an implementation and evaluation of the protocol on Nexus One smart phones and demonstrates that the protocol is practical.

III. Problem Definition

In HealthCare Social Network's conflicts occur with users growing privacy concerns about disclosing user's personal profiles to strangers before deciding to interact with them. To limit the risk of privacy exposure the existing systems uses two approaches.

- ➢ Disclosing minimal and necessary personal information to as few users as possible.
- ➢ The second approach requires a trusted server that knows the interests and current location of each user and performs matchmaking based on this information.

A. Objective

In this work, the challenges in existing system are overcome by making the following main contributions:

1. 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.

2. Two fully distributed privacy-preserving Profile matching schemes have been defined, one of them being a private set intersection (PSI) protocol and the other is a private cardinality of set-intersection (PCSI) protocol.

B. *Privacy Risks*

HEALTHCARE SOCIAL NETWORK'S may have a number of privacy and security issues. First, the site may maintain a vast repository of users' profiles and keep it permanently. The content produced by users may be revealed to both intended and unintended audiences. Since anybody can register on the website, anybody can view the content on the site. For example, any person or entity may create fake accounts in order to obtain data from unsuspecting users. Another related issue is that the website may exchange data with third parties without explicit consent. The accumulated health data can be misused and/or exploited for various non-medical uses. Some HEALTHCARE SOCIAL NETWORK'S are commercial companies that have a business model based on harvesting health data for business and proprietary purposes. Another obvious issue is the scale of the security risk.

C. *Privacy Policies*

The amount of the data shared by users is positively correlated with their experiences of risks. The more data users share, the more risks they encounter, users may not provide personally identifiable information (PII) such as their real name and national identification number. Yet, users often share many more personal details on HEALTHCARE SOCIAL NETWORK'S than they would otherwise because complete information is pivotal for effective health care.

IV. Methodology

The methodology defines two protocols that aim at realizing one level of privacy requirement each. Starting with the basic scheme realizing private setintersection (PSI) protocol under Privacy Level-1, which is based on secure polynomial evaluation using secret sharing.

PSI consists of two algorithms: {Setup; Interaction} Setup: a process wherein all global/public parameters are selected. Interaction: a protocol between client and server that results in the client obtaining the intersection of two sets. At a high level, for P1 and each Pi ($2 \leq i \leq N$), their inputs are shared among a subset Pi of 2t + 1 parties, based on which they cooperatively compute shares. To reduce the communication complexity, an enhancement is defined that aggregates multiple multiplication and addition operations into one round during the secure polynomial evaluation computation.

For Privacy Level-2, the advanced scheme achieves efficient private cardinality of set-intersection (PCSI) protocol. The main idea is that, the parties in Pi first compute the (t, 2t+1) shares securely using the basic scheme, then the best matched profile is given as output.

Security Properties

The below section describes security requirements for PSI.

- **Correctness** A PSI scheme is correct if, at the end of Interaction, client outputs the exact (possibly empty) intersection of the two respective sets.
- **Server Privacy** Informally, a PSI scheme is server-private if the client learns no information (except the upperbound on size) about the subset of elements on the server that are NOT in the intersection of their respective sets.
- **Client Privacy** Informally, client privacy (in either PSI or APSI) means that no information is leaked about client's set elements to a malicious server, except the upper bound on the client's set size.

V. Implementation

For the implementation of the schemes the scenario considered in this work is an online healthcare social network for patients profile matching. 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 those 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.

In this scenario, two fully-distributed privacy preserving profile matching protocols have been defined, without relying on neither a client-server relationship nor any central server. Homomorphic properties of Shamir secret sharing are exploited to compute the intersection between user profiles privately, and due to the smaller computational domain of secret sharing, the protocols can achieve higher performance and lower energy consumption for practical parameter settings of an HEALTHCARE SOCIAL NETWORK'S .

VI. Conclusion

The growing use of HEALTHCARE SOCIAL NETWORK'S presents significant risk for individual privacy. Users themselves play a critical role in helping to safeguard their own data. However, users often are often unaware of the risk and do not have the skills and ability to protect their privacy. The provider is reluctant to offer protections because they may reduce the benefits of open communication and data sharing. But even if privacy mechanisms were built into the platform and even if users were aware and competent in optimizing their privacy settings, users would still be exposed to potential privacy violations by the provider and its partners

A. *Future Work*

The scheme defined is only proven under distributed environment; 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. The authentication can be made strong by providing an option for e-mail verification and phone number verification to avoid identity thefts.

REFERENCES

[1] Lan Zhang, Xiang-Yang Li, Yunhao Liu “Message in a Sealed Bottle: Privacy Preserving Friending in Social Networks” in IEEE ICDCS 2013

[2] Qi Xie and Urs Hengartner “Privacy-Preserving Matchmaking For Mobile Social Networking Secure Against Malicious Users” in IEEE 2011

[3] M. Li, N. Cao, S. Yu, and W. Lou, “Findu: Privacy-preserving personal profile matching in mobile social networks,” in IEEE INFOCOM Apr 2011

[4] W. Dong, V. Dave, L. Qiu, and Y. Zhang, “Secure friend discovery in mobile social networks,” in IEEE INFOCOM ’11, Apr 2011

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

[6] E. De Cristofaro, A. Durussel, and I. Aad, “Reclaiming privacy for smartphone applications,” in Pervasive Computing and Communications (PerCom), 2011 IEEE International Conference on, march 2011

[7] 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 June 2010

[8] E. D. Cristofaro and G. Tsudik, “Practical private set intersection protocols with linear complexity” in Financial Cryptography and Data Security 2010

[9] D. Dachman-Soled, T. Malkin, M. Raykova, and M. Yung, “Efficient robust private set intersection,” in ACNS ’09, 2009

[10] 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