e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

International Journal Of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704149 |

Privacy-Preserving User Profile Matching In Social Networks

M.BUVANESHWARI, Dr.KANNAN, NARESH M, MUTHUPANDI R, JAYANTH G,

Assistant Professor, Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

Professor, Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

ABSTRACT: Photo sharing is an attractive feature which popularizes Online Social Networks (OSNs). Unfortunately, it may leak user's privacy if they are allowed to post, comment, and tag a photo freely. In this paper we try to implement the security of our current OSN with three main scenarios like: An image which is uploaded in public profile will be accessed only by the direct friends or family members of that posted user, which is not allowed or accessed by friends of friends or family of family members. In the second scenario we try to give security for the private profile sharing by restricting the users not to access private content by all members who are mutually related. In the third scenario we try to give security for the comments posted for the images by several individuals. Now a day's all the comments can be viewed by each and every one who is connected with that profile, but in our proposed application we try to provide security by restricting un known persons not to access or read others comments posted on user image. We show that our system is superior to other possible approaches in terms of recognition ratio and efficiency. Our mechanism is implemented as a proof to enable more security for the social network sites to share the data among several users.

KEYWORDS: Privacy, Security, Restriction, Online Social Networks, Profile Sharing.

I.INTRODUCTION

Online social networks (OSNs) such as Facebook, Google+, and Twitter are inherently designed to enable people to share personal and public information and make social connections with friends, coworkers, colleagues, family and even with strangers. In recent years, we have seen unprecedented growth in the application of OSNs. For example, Facebook, one of representative social network sites, claims that it has more than 800 million active users and over 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each month. To protect user data, access control has become a central feature of OSNs a typical OSN provides each user with a virtual space containing profile information, a list of the user's friends, and web pages, such as wall in Facebook, where users and friends can post content and leave messages.

A user profile usually includes information with respect to the user's birthday, gender, interests, education and work history, and contact information. In addition, users can not only upload content into their own or others' spaces but also tag other users who appear in the content. Each tag is an explicit reference that links to a user's space. For the protection of user data, current OSNs indirectly require users to be system and policy administrators for regulating their data, where users can restrict data sharing to a specific set of trusted users. OSNs often use user relationship and group membership to distinguish between trusted and untrusted users.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704149 |

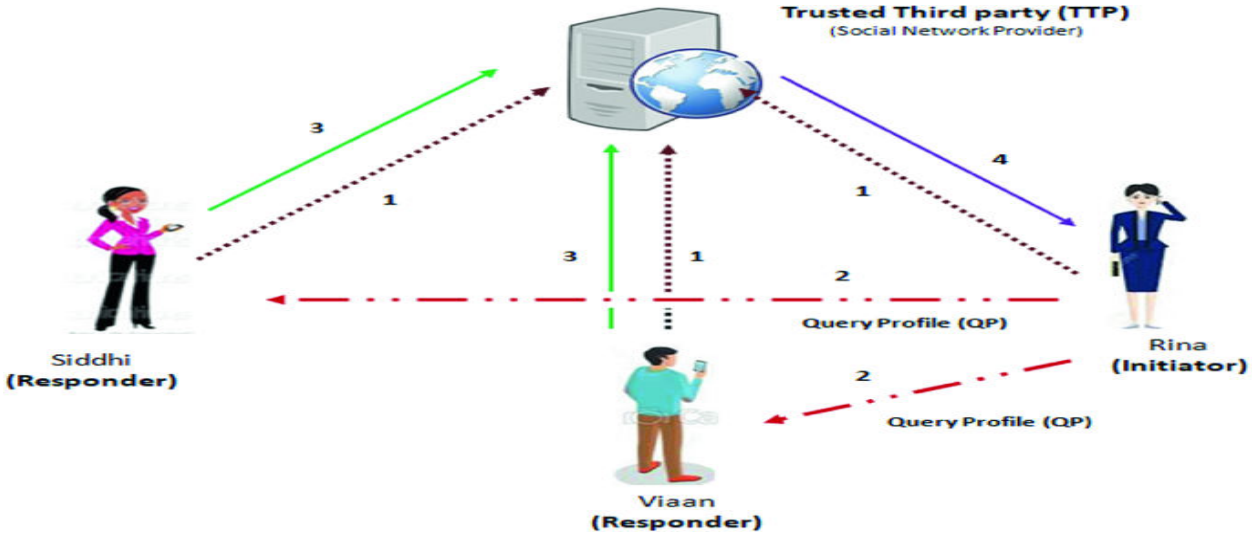

Fig 1: Privacy Preserving Profile Matching in Mobile Social Network

For example, in Facebook, users can allow friends, friends of friends, groups or public to access their data, depending on their personal authorization and privacy requirements. The existing work could model and analyze access control requirements with respect to collaborative authorization management of shared data in OSNs. The need of joint management for data sharing, especially photo sharing, in OSNs has been recognized by the recent work provided a solution for collective privacy management in OSNs. Their work considered access control policies of a content that is co-owned by multiple users in an OSN, such that each co-owner may separately specify her/his own privacy preference for the shared content.

II.LITERATURE SURVEY

Photo sharing is an attractive feature which popularizes Online Social Networks (OSNs). Unfortunately, it may leak users' privacy if they are allowed to post, comment, and tag a photo freely. In this paper, we attempt to address this issue and study the scenario when a user shares a photo containing individuals other than himself/herself (termed co-photo for short). To prevent possible privacy leakage of a photo, we design a mechanism to enable each individual in a photo be aware of the posting activity and participate in the decision making on the photo posting. For this purpose, we need an efficient facial recognition (FR) system that can recognize everyone in the photo. However, more demanding privacy setting may limit the number of the photos publicly available to train the FR system. To deal with this dilemma, our mechanism attempts to utilize users' private photos to design a personalized FR system specifically trained to differentiate possible photo co-owners without leaking their privacy. We also develop a distributed consensus based method to reduce the computational complexity and protect the private training set. We show that our system is superior to other possible approaches in terms of recognition ratio and efficiency. Our mechanism is implemented as a proof of concept Android application on Facebook's platform.

This article examines privacy as a generic process that occurs in all cultures but that also differs among cultures in terms of the behavioral mechanisms used to regulate desired levels of privacy. Ethnographic data are examined from a variety of cultures, particularly from societies with apparently maximum and minimum privacy, and from analyses of various social relationships, such as parents and children, in-laws, husbands and wives. It is concluded that privacy is a universal process that involves culturally unique regulatory mechanisms. in a system and expressive conditions in access control policy rules, it can be very challenging for security administrators to envision what can (or cannot) happen as the protection system evolves. In this paper, we introduce the security analysis problem for this class of policies, where we seek to answer security queries about future states of the system graph and authorizations that are decided accordingly. Towards achieving this goal, we propose a state-transition model of a ReBAC protection system, called RePM. We discuss about formulation of security analysis queries in RePM and present our initial results for a limited version of this model.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704149 |

III.METHODS

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 cellphone 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] proposed a symptom matching scheme for mobile health social networks, assuming the existence of a semi-online central authority.

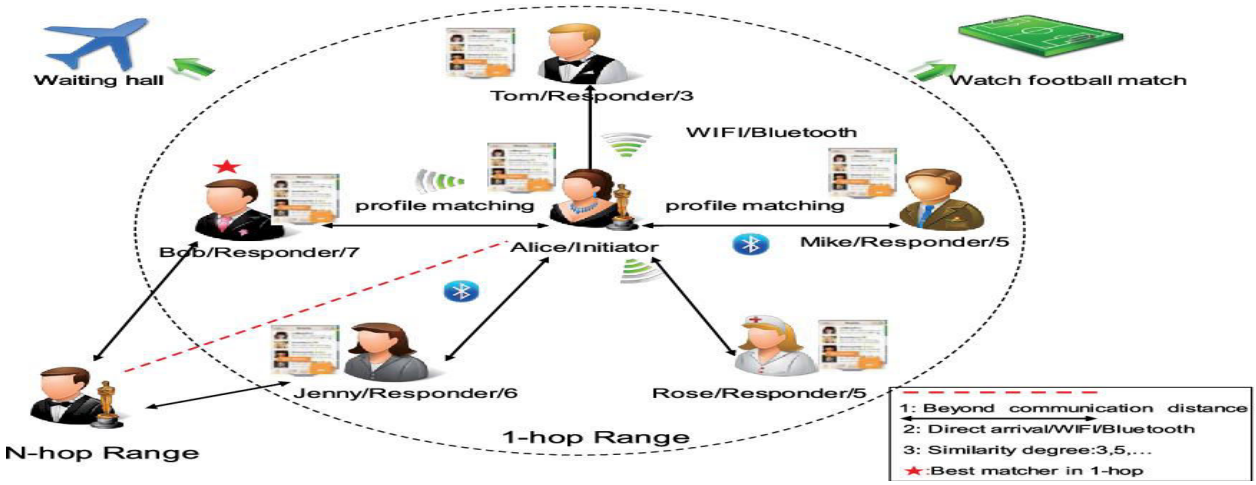

Fig 2: Privacy-preserving multi-hop profile-matching

Concurrently with our work, a secure friend discovery protocol has been proposed in [14]. Different from us, their matching is based on computing the similarity (dot product) between two users' coordinates (which is not as intuitive as the intersection of the profile attributes as ours). In addition, a centralized trusted authority is needed to provide the coordinates. In [15], a private contact discovery protocol is proposed, where contact list manipulation is prevented by distributed certification. However, for general sensitive profile attributes it is difficult to find a distributed certifier in practice, whereas our protocols are not limited in the type of attributes to share with. In [16], privacy-preserving multi-party interest sharing protocols for smartphone applications are proposed.

We propose two fully-distributed privacypreserving profile matching protocols, without relying on a client-server relationship nor any central server. We propose novel methods to reduce energy consumption and protocol run time, while achieving reasonable security levels. Specifically, we exploit the homomorphic properties of Shamir secret sharing to compute the intersection between user profiles privately, and due to the smaller computational domain of secret sharing, our protocols achieve higher performance and lower energy consumption for practical parameter settings of an MSN. Such a framework is also applicable to many scenarios beyond the motivating problems in this paper, for example, in patient matching in online healthcare social networks.

IV.RESULT ANALYSIS

In the honest-but-curious model, an external adversary and an internal adversary are considered. An external adversary mainly refers to an eavesdropper who can get some information (e.g., encrypted data) through the transparent channel by eavesdropping. An internal adversary is an honest-but-curious entity such that he faithfully follow the agreement but attempt to collect and reveal private information during the execution of the agreement. The friend finder may want to expose other users' profiles, while the two clouds may want to reveal the users' personal data in the social networks.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704149 |

Moreover, it is assumed that the two clouds will never collude with each other and the users will not deliberately attempt to guess the cosine result by adjusting the vector multiple times.

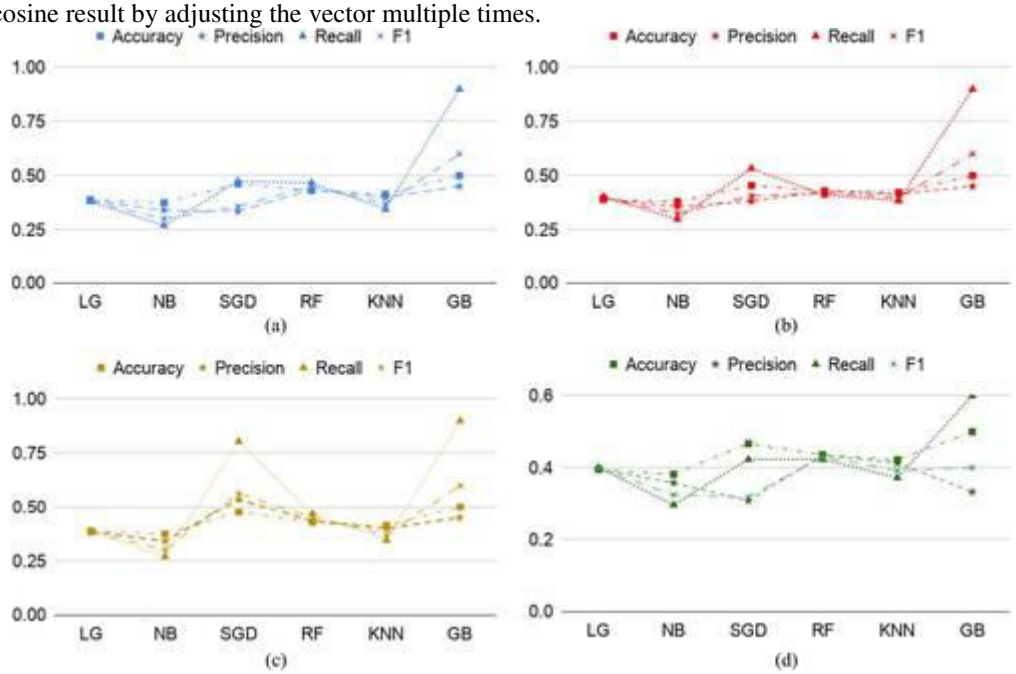

Fig 3: Optimizing user profile matching

In this subsection, we mainly discuss the advantages of our scheme compared with the existing privacy-preserving profile-matching schemes in require users to stay online simultaneously to obtain matching results through multiple interactions, resulting in additional computational costs and communication overheads on mobile devices of users. In our scheme, users only need to encrypt their personal profiles and upload them to the cloud, and then they can go offline. For a Friend finder, he can designate a target to initiate a matching query and ultimately get the matching result. Most computations are undertaken by the two cloud servers, which can greatly reduce the burden of users. Compared with the scheme in [2], the users do not need to upload the re-encryption keys when uploading their encrypted data, thereby avoiding the risk of the users' personal data leakage due to the re-encryption key leakage and reducing the burden of the key management. We use the cosine scores of two vectors as the matching result instead of the intersection of two sets or the inner product of two vectors. In particular, the proposed scheme supports processing larger data.

V.CONCLUSION

In this paper, we propose a privacy-preserving profile-matching scheme over improved HRES algorithm in mobile social networks. The improved algorithm can support one-time homomorphic multiplication and arbitrarily many homomorphic additions. Compared with the original scheme [2], the key management burden can be reduced, and the privacy problem of users caused by the re-encryption keys leakage can be effectively solved. In addition, our scheme utilizes the cosine result between two normalized vectors as the standard for measuring the users' proximity, which can effectively improve the social experience of the users. Even if users with ulterior motives collude with one of the clouds, the personal data of other users will not be revealed. At last, we prove that our scheme is secure under the semihonest model through strict security analysis.

REFERENCES

1. R. Zhang, J. Zhang, Y. Zhang, J. Sun, and G. Yan, "Privacy-preserving profile matching for proximity-based mobile social networking," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 656–668, 2013.
View at: Publisher Site | Google Scholar
2. C. Gao, Q. Cheng, X. Li, and S. Xia, "Cloud-assisted privacy-preserving profile-matching scheme under multiple keys in mobile social network," *Cluster Computing*, vol. 22, no. 1, pp. 1655–1663, 2019.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704149 |

View at: Publisher Site | Google Scholar

3. I. Ioannidis, A. Grama, and M. Atallah, "A secure protocol for computing dot-products in clustered and distributed environments," in *Proceedings of the International Conference on Parallel Processing*, pp. 379–384, IEEE, Washington, DC, USA, September 2002.
   View at: Google Scholar
4. A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes," *ACM Computing Surveys*, vol. 51, no. 4, pp. 1–35, 2018.
   View at: Publisher Site | Google Scholar
5. C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, pp. 169–178, Bethesda, MD, USA, May 2009.
   View at: Google Scholar
6. C. Gentry, A. Sahai, and B. Waters, "Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based," in *Proceedings of the Annual International Cryptology Conference*, pp. 78–92, Santa Barbara, CA, USA, August 2013.
   View at: Google Scholar
7. Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," *SIAM Journal on Computing*, vol. 43, no. 2, pp. 831–871, 2014.
   View at: Publisher Site | Google Scholar
8. D. Boneh, C. Gentry, S. Halevi, F. Wang, and D. J. Wu, "Private database queries using somewhat homomorphic encryption," in *Proceedings of the International Conference on Applied Cryptography and Network Security*, pp. 102–118, Banff, AB, Canada, June 2013.
   View at: Publisher Site | Google Scholar
9. L. Morris, *Analysis of Partially and Fully Homomorphic Encryption*, Rochester Institute of Technology, Rochester, NY, USA, 2013.
10. L. Zhang, X. Y. Li, Y. Liu, and T. Jung, "Verifiable private multiparty computation: ranging and ranking," in *Proceedings of the 2013 IEEE INFOCOM*, pp. 605–609, IEEE, Turin, Italy, 2013.
    View at: Google Scholar
11. W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in *Proceedings of the 2011 IEEE INFOCOM*, pp. 1647–1655, IEEE, Shanghai, China, 2011.
    View at: Google Scholar

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com