ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

An Multipath Knowledge Based Search Algorithm for User Profile Matching

R.Karthikeyan[1], V.Khanna[2]

[1]Assitant Professor, Department of Computer Science Engineering, Bharath University, Chennai, India

[2]Dean, Department of Information Technology, Bharath Univeristy, Chennai, India

ABSTRACT: The usage of hand-held devices has created analysis activity into new protocols and applications that may handle and exploit the shaping characteristic of this new atmosphere user quality. additionally to quality, another shaping characteristic of mobile systems is user social interaction. To Explore the Threats to privacy that arises once users of privacy awareness and concern in information transfer websites. Profile matching refers to 2 users comparison their personal profiles. It Conflicts with user's growing privacy concern regarding revealing their personal profiles to complete strangers. The Protocols modify 2 users to perform profile matching while not revealing any data regarding their profiles on the far side the comparison result,Making new connections consistent with personal preferences could be a crucial service in mobile social networking, wherever associate initiating user will realize matching users inside physical proximity of him/her. The survey is regarding matching protocols that modify associate initiating user to search out from a gaggle of users the one whose profile best matches with his/her to limit the danger of privacy exposure, solely necessary and lowest data regarding the personal attributes Of the collaborating users is changed.

KEYWORDS: Mobile social network, profile matching, privacy preservation, homomorphic encryption, oblivious transfer.

I. INTRODUCTION

Social networking makes digital communication technologies sharpening tools for extending the social circle of people. It has already become an important integral part of our daily lives, enabling us to contact our friends and families on time. As reported by ComScore social networking sites such as Face book and Twitter have reached 82 percent of the world online population, representing 1.2 billion users around the world. In the meantime, fueled by the pervasive adoption of advanced handheld devices and the ubiquitous connections of Bluetooth/Wi-Fi/GSM/LTE networks, the use of Mobile Social Networking (MSNs) has surged. In the MSNs, users are able to not only surf the Internet but also communicate with peers in close vicinity using short-range wireless communications. Due to its geographical nature, the MSNs support many promising and novel applications. For example, through Bluetooth communications, People Net enables efficient information search among neighboring mobile phones; a message-relay approach is suggested in to facilitate carpool and ride sharing in a local region. Realizing the potential benefits brought by the MSNs, recent research efforts have been put on how to improve the effectiveness and efficiency of the communications among the MSN users.

They developed specialized data routing and forwarding protocols associated with the social features exhibited from the behavior of users, such as, social friendship, social selfishness and social morality. It is encouraging that the traditional solutions can be further extended to solve the MSN problems by considering the unique social features. Privacy preservation is a significant research issue in social networking. Since more personalized information is shared with the public, violating the privacy of a target user become much easier. Research efforts have been put on identity presentation

DOI: 10.15680/IJIRSET.2014.0311115

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

and privacy concerns in social networking sites. Gross and Acquisti argued that users are putting themselves at risk both offline (e.g., stalking) and online (e.g., identity theft) based on a behavior analysis of more than 4,000 students who have joined a popular social net- working site. Stutzman presented a quantitative analysis of identity information disclosure in social network communities and subjective opinions from students regarding identity protection and information disclosure. When the social networking platforms are extended into the mobile environment, users require more extensive privacy-preservation because they are unfamiliar with the neighbors in close vicinity who may eavesdrop, store, and correlate their personal information at different time periods and locations. Once the personal information is correlated to the location information, the behavior of users will be completely disclosed to the public. Chen and Rahman surveyed various mobile Social Networking Applications (SNAs), such as, neighborhood exploring applications, mobile-specific SNAs, and content-sharing applications, all of which provide no feedback or control mechanisms to users and may cause inappropriate location and identity. To overcome the privacy violation in MSNs, many privacy enhancing techniques have been adopted into the MSN applications. For example, when two users encounter in the MSNs, privacy-preserving profile matching acts as a critical initial step to help users, especially strangers, initialize conversation with each other in a distributed and privacy-preserving manner. Many research efforts on the privacy preserving profile matching have been carried out. The common goal of these works is to enable the handshake between two encountered users if both users satisfy each other's requirement while eliminating the unnecessary information disclosure if they are not. The original idea is from [18], where an agent of the Central Intelligence Agency (CIA) wants to authenticate herself to a server, but does not want to reveal her CIA credentials unless the server is a genuine CIA outlet. In the meantime, the server does not want to reveal its CIA credentials to anyone but CIA agents.

In the MSNs, we consider a generalized function to support information exchange by using profile matching as a metric.

Following the previous example, we consider two CIA agents with two different priority levels in the CIA system, A with a low priority lA and B with a high priority lB. They know each other as a CIA agent. However, they do not want to reveal their priority levels to each other. B wants to share some messages to A. The messages are not related to user profile, and they are divided into multiple categories, e.g., the messages related to different regions (New York or Beijing) in different years (2011 or 2012). B shares one message of a specified category T at a time. The category T is chosen by a, but the choice is unknown to B. For each category, B prepares two self-defined messages, e.g., a low-confidential message for the CIA agent at a lower level and a high-confidential message for the agent at a higher level. Because lA < lB, A eventually obtains the low-confidential message without knowing that it is a low-confidential one. In the meantime, B does not know which message A receives. The above function offers both A and B the highest anonymity since neither the comparison result between lA and lB is disclosed to A or B nor the category T of A's interest is disclosed to B. In the following, we refer to A as the initiator ui, B as the responder uj, the attribute used in the comparison (i.e., priority level) as ax, and the category T of A's interest as Ty. The attribute values of ui and uj on the attribute ax are denoted by ai,x and aj,x respectively.

We first formally describe two scenarios from the above examples. Scenario-1: The initiator wants to know the comparison result, i.e., whether it has a value larger, equal, or smaller than the responder on a specified attribute. The initiator ui expects to know if ai, x > aj, x, ai, x = aj, x, or ai, x < aj,x. Scenario-2: The initiator expects that the responder shares one message related to the category of its interest, which is however kept unknown to the responder. In the meantime, the responder wants to share with the initiator one message which is determined by the comparison result of their attribute values. For example, as shown in Fig. 1 (b), both ui and uj know that ax is used in the comparison and the categories of messages are T1, ··, Tλ. The initiator ui first generates a (0, 1)-vector where the y-th dimension value is 1 and other dimension values are 0. Then, ui encrypts the vector with its own public key and sends cipher texts (E (0), ···, E (1), ···, E (0)) to the responder uj. The cipher texts imply ui's interested category Ty, but uj is unable to know Ty since E (0) and E

DOI: 10.15680/IJIRSET.2014.0311115

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

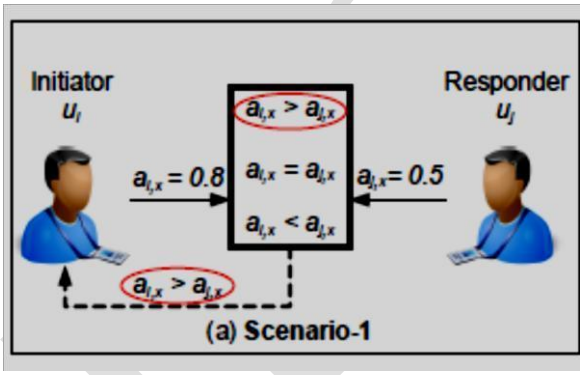
(1) are non distinguishable without a decryption key.

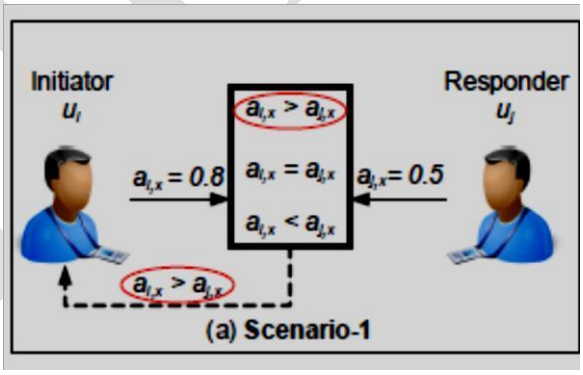
Ui also provides its attribute value ai, x in an encrypted form so that uj is unable to obtain ai, x. On the other hand, uj prepares λ pairs of messages, each pair (s1, h, s0, h) relating to one category The ($1 \leq h \leq \lambda$). uj executes a calculation over the cipher text and sends the result to ui. Finally, ui obtains E(s1,y) if ai,x > aj,x or E(s0,y) if ai,x < aj,x, and obtains s1,y or s0,y by the decryption.

Definition 1 (Non-Anonymity). A profile matching protocol Provides non-anonymity if after executing multiple runs of the Protocol with any user, the probability of correctly guessing the profile of the user is equal to 1.

Definition 2 (Conditional Anonymity). A profile matching Protocol achieves conditional anonymity if after executing Multiple runs of the protocol with some user, the probability of correctly guessing the profile of the user is larger than 1

Definition 3(Full Anonymity). A profile matching protocol Achieves full anonymity if after executing multiple runs of the Protocol with any user, the probability of correctly guessing The profile of the user is always 1/v.





DOI: 10.15680/IJIRSET.2014.0311115

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

II. OUR CONTRIBUTIONS

In this paper, we propose a family of novel protocols eCPM, iCPM, and iPPM to solve the considered profile matching Problems based on the above network model. These protocols rely on the homomorphic encryption to protect the content of user profiles from disclosure. They provide increasing levels of anonymity (from conditional to full). Our contributions are summarized below. Firstly, we propose the eCPM for Scenario-1. For a specified attribute, the eCPM allows the initiator to know the comparison result, i.e., whether it has a larger, equal, or smaller value than the responder on the attribute. Due to the exposure of the comparison result, user profile will be leaked and linked in some conditions. We provide a numerical analysis on the conditional anonymity of the eCPM. We study the anonymity risk level in relation to the pseudonym change for the consecutive eCPM runs. Secondly, we propose the iCPM for Scenario-2. In this protocol, the responder prepares multiple categories of messages where two messages are generated for each category. The initiator can obtain only one message related to one category for each run. During the protocol, the responder is unable to know the category of the initiator's interest. To receive which message in the category is dependent on the comparison result on a specified attribute. The responder does not know which message the initiator receives, while the initiator cannot derive the comparison result from the received message. We provide an analysis of the effectiveness of the iCPM, and show that the iCPM achieves full anonymity. Thirdly, we extend the iCPM to obtain the iPPM, which has the same anonymity property as the iCPM. The iPPM allows the comparisons of multiple attributes for profile matching. The responder defines a predicate, similar to which is a logical expression made of multiple comparisons between its own attribute values and the initiators attribute values. The initiator receives one message from the responder corresponding to the specified category.[1] To receive which message in the category is dependent on whether the initiator's attribute Values satisfy the predicate or not. We provide an analysis of the effectiveness of the iPPM. Fourthly, we improve the eCPM by combining it with an adaptive pseudonym change strategy and obtain a new variant eCPM+. In the eCPM+, each user measures its current neighborhood status periodically and predicts its future Neighborhood status using an Autoregressive Moving Average (ARMA) model. Based on the aggregate neighborhood status Since last pseudonym change, it periodically estimates its anonymity risk level and changes its pseudonym when the Level is too high. The extensive trace-based simulation shows that eCPM+ achieves significantly higher anonymity strength With slightly larger number of used pseudonyms than the eCPM. The remainder of this paper is organized as follows. We review existing profile matching protocols in Sec. II and introduce some fundamental techniques in Sec. III. The three protocols eCPM, iCPM, and iPPM are presented respectively in Sec. IV-VI, along with the effectiveness discussion. Their Communication overhead and anonymity strength are analyzed in Sec. VII. We present the eCPM+ in Sec. VIII and evaluate Its performance in Sec. IX. Finally, we conclude the paper in Sec. X.

III. RELATED WORK

Mobile social networks as emerging social communication Platforms have attracted great attention recently, and their mobile applications have been developed and implemented pervasively.[2] In mobile social networking applications, profile matching acts as a critical initial step to help users,especially strangers, initialize conversation with each other in a distributed manner[4]. Yang et al. introduced a distributed Mobile communication system, called E-Small Talker, which facilitates social networking in physical proximity. ESmall Talker automatically discovers and suggests common topics between users for easy conversation. Studied e-healthcare cases by proposing a symptom matching Scheme for mobile health social networks. They considered that such matching scheme is valuable to the patients who have the same symptom to exchange their experiences, mutual support, and inspiration with each other. In general, the profile matching can be categorized based on the formats of profiles and the types of matching operations.[5] A well-known profile matching is the FNP scheme, where a client and a server compute their intersection set such that the client gets the result while the server learns nothing. Later, Kissner et al.implemented profile matching with more operations including set intersection, union, cardinality and over-threshold operations. On the other hand, Ye et al. further extended the FNP scheme to a distributed

DOI: 10.15680/IJIRSET.2014.0311115

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

private matching scheme and Dachman-Soled et al. aimed at reducing the protocol complexity[6]. All the above solutions to the set intersection rely on homomorphic encryption operation. In the meantime, other works employed an oblivious pseudo random function to build their profile matching protocols, where communication and computational efficiency is improved. Li et al implemented profile matching according to three increasing privacy levels: i) revealing the common attribute set of the two users; ii) revealing the size of the common attribute set; and iii) revealing the size rank of the common attribute sets between a user and its neighbors. They considered an honest-but-curious (HBC) adversary model, which assumes that users try to learn more information than allowed by inferring from the profile matching results, but honestly following the protocol.[7] They applied secure multiparty computation, the Shamir secret sharing scheme, and the homomorphic encryption scheme to achieve the confidentiality of user profiles. In another category of profile matching profiles can be represented as vectors, and matching operation can be inner product or distance[8]. Such profile matching is a special instance of the secure two-party computation, which was initially introduced by Yao and later generalized to the secure multi-party computation by Goldreich et al. specifically; we introduce two recent works in this category. Dong et il-considered user profile consisting of attribute values and measured the proximity of two user profiles using Dot product fdot (u, v). An existing dot product protocol is improved to enable verifiable secure computation. The improved protocol only reveals whether the dot product is above or below a given threshold. The threshold value is selected by the user who initiates the profile matching. They pointed out the potential anonymity risk of their protocols; an adversary May adaptively adjust the threshold value to quickly narrow down the value range of the victim profile. Thus, it is required that the threshold value must be larger than a pre-defined lower bound (a system parameter) to guarantee user anonymity.[9]

IV.CONCLUSION

We have investigated a unique comparison-based profile matching problem in Mobile Social Networks (MSNs), and proposed novel protocols to solve it. The explicit Comparison based Profile Matching (eCPM) protocol provides conditional Anonymity. It reveals the comparison result to the initiator. Consider the k-anonymity as a user requirement; we analyze the anonymity risk level in relation to the pseudonym change for consecutive eCPM runs. We have further introduced a enhanced version of the eCPM, i.e., eCPM+, by exploiting the prediction-based strategy and adopting the pre-adaptive pseudonym change. The effectiveness of the eCPM+ is validated through extensive simulations using real-trace data. We have also devised two protocols with full anonymity, i.e., implicit Comparison-based Profile Matching (iCPM) and implicit Predicate-based Profile Matching (iCPM). The ICPM handles profile matching based on a single comparison of an attribute while the iPPM is implemented with a logical expression made of multiple comparisons spanning multiple attributes. The iCPM and the iPPM both enable users to anonymously request for messages and respond to the requests according to the profile matching result, without disclosing any profile information. In current version of the iCPM and the iPPM, we implement “>” and “<” operations for profile matching. One future work is to extend them to support more operations, such as “≥” and “≤”. Another future work is to hide the predicate information in the iPPM. Currently, the responder needs to transmit the threshold value of the predicate to the initiator, which may reveal partial information of the responder’s interest. Restricting the disclosure of such parameter will be of significance for advancing comparison-based family of profile matching protocols and warrants deep investigation.

REFERENCES

1. Kaliyamurthie K.P., Parameswari D., Udayakumar R., "QOS aware privacy preserving location monitoring in wireless sensor network", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S5) (2013) pp.4648-4652.

2. “Analyzing privacy designs of mobile social networking applications,” ieee/ifip international conference on embedded and ubiquitous computing, g. chen and f. Rahman, vol. 2, pp. 83–88, 2008.

DOI: 10.15680/IJIRSET.2014.0311115

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

3. Sharmila D., Muthusamy P., "Removal of heavy metal from industrial effluent using bio adsorbents (Camellia sinensis)", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 5(2) (2013) pp.10-13.

4. Secure friend discovery in mobile social networks," in proc. ieee infocom, w. dong, v. dave, l. qiu, andy. zhang 2011, pp. 1647– 1655.

5. Udayakumar R., Khanaa V., Saravanan T., Saritha G., "Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction", Middle - East Journal of Scientific Research, ISSN : 1990-9233, 16(12) (2013) pp.1781-1785.

6. "morality- driven data forwarding with privacy preservation in mobile social networks," ieee transactions on vehicular technology, x. liang, x. li, t. h. luan, r. lu, x. lin, and x. shen, vol. 7, no. 61, pp. 3209–3222, 2012.

7. Kalaiselvi V.S., Prabhu K., Ramesh M., Venkatesan V., "The association of serum osteocalcin with the bone mineral density in post menopausal women",Journal of Clinical and Diagnostic Research, ISSN : 0973 - 709X, 7(5) (2013) pp.814-816.

8. exploiting friendship relations for efficient routing in delay tolerant mobile social networks," ieee transactions on parallel and distributed systems, E.Bulut and B.Szymanski, vol. 23, no. 12, pp. 2254–2265, 2012.

9. Jayalakshmi T., Krishnamoorthy P., Kumar G.R., Sivamani P., "The microbiologicalquality of fruit containing soft drinks from Chennai", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 3(6) (2011) pp. 626-630.

10.Dr.A.Muthu Kumaravel, KNOWLEDGE BASED WEB SERVICE, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,pp 5881-5888, Vol. 2, Issue 9, September 2014

11.Dr.A.Muthu Kumaravel, Data Representation in web portals, International Journal of Innovative Research in Computerand Communication Engineering, ISSN(Online): 2320-9801,pp 5693-5699, Vol. 2, Issue 9, September 2014

12.Dr.Kathir.Viswalingam, Mr.G.Ayyappan,A Victimization Optical Back Propagation Technique in Content Based Mostly Spam Filtering ,International Journal of Innovative Research in Computer and Communication Engineering ,ISSN(Online): 2320-9801 , pp 7279-7283, Vol. 2, Issue 12, December 2014

13.Kannan Subramanian,FACE RECOGNITION USINGEIGENFACE AND SUPPORT VECTOR MACHINE,International Journal of Innovative Research in Computerand Communication Engineering,ISSN(Online): 2320-9801,pp 4974-4980, Vol. 2, Issue 7, July 2014.

14.Vinothlakshmi.S,To Provide Security & Integrity for StorageServices in Cloud Computing ,International Journal of Innovative Research in Computer and Communication Engineering ,ISSN(Online): 2320-9801 , pp 2381-2385 ,Volume 1, Issue 10, December 2013

DOI: 10.15680/IJIRSET.2014.0311115