ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 148-151 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

Efficient Distributed Profile Matching Using Multi-Party Computation in Mobile Social Networks

V.Himabindu

M.Tech Student, Dept of CSE, St. Ann's College of Engineering & Technology, Chirala, Prakasam Dist, A.P, India

Dr. P. Harini

Professor and HOD Dept of CSE, St. Ann's College of Engineering & Technology, Chirala, Prakasam Dist, A.P, India

ABSTRACT:*The Profile matching means that 2 users scrutiny their personal profiles and is usually the primary step towards effective PMSN. It, however, conflicts with users' growing privacy considerations regarding revealing their personal profiles to finish strangers before deciding to move with them Our protocols alter 2 users to perform profile matching while not revealing any info regarding their profiles on the far side the comparison resul creating new connections in keeping with personal preferences could be a crucial service in mobile social networking, wherever associate degree initiating user will notice matching users inside physical proximity of him/her. In existing systems for such services, typically all the users directly publish their complete profiles for others to look. However, in several applications, the users' personal profiles could contain sensitive info that they are doing not wish to create public. during this paper, we have a tendency to propose FindU, a group of privacy-preserving profile matching schemes for proximity-based mobile social networks. In FindU, associate degree initiating user will notice from a gaggle of users the one whose profile best matches with his/her; to limit the danger of privacy exposure, solely necessary and negligible info regarding the non-public attributes of the collaborating users is changed. 2 increasing levels of user privacy area unit outlined, with decreasing amounts of disclosed profile info. Leverage secure multi-party computation (SMC) techniques, we have a tendency to propose novel protocols that understand every of the user privacy levels, which may even be customized by the users. We offer formal security proofs and performance analysis on our schemes, and show their blessings in each security and potency over progressive schemes. The social proximity between 2 users because the matching metric, that measures the space between their social coordinates with every being a vector pre computed by a trustworthy central server to represent the situation of a user in an internet social network. By comparison, our work doesn't admit the affiliation of PMSN users with one on-line social network and addresses a lot of general non-public matching downside for PMSN by supports fine-grained personal profiles and a good spectrum of matching metrics.*

Keywords: Social network, Privacy, Profile matching metrics.

INTRODUCTION:

With the proliferation of mobile devices, mobile social networks (MSNs) are getting associate indivisible a part of our lives. Leveraging networked transportable devices like sensible phones and PDAs as platforms, MSN not solely permits folks to use their existing on-line social networks (OSNs) at anyplace and anytime, however additionally introduces a myriad of mobility-oriented applications, like location-based services and increased reality. Among them, a vital service is to create new social connections friends inside physical proximity supported the matching of private profiles. as an example, MagnetU and E-SmallTalker [2] area unit MSN applications that match one with nearby folks for geological dating or friend-making supported common interests. In such associate application, a user solely has to input some (query) attributes in her profile, and also the system would automatically notice the persons around with similar profiles. The scopes of those applications area unit terribly broad, since folks can input something as they require, like hobbies, phone contacts and places they need been to. The latter will even be accustomed notice "lost connections" and "familiar strangers". However, such systems additionally raise variety of privacy issues. Let us 1st examine a noteworthy situation. in an exceedingly hospital, patients could embody their ill health symptoms and medications in their personal profiles so as to search out similar patients, for physical or mental support. During this situation, associate initiating user (initiator) might want to search out the patient having the maximum range of identical symptoms together with her, whereas being reluctant to disclose her sensitive ill health data to the remainder of the users, and also the same for the users being matched with. If users' personal profiles area unit directly changed with one another, it will facilitate user identification wherever those data will be simply collected by a close-by user, either in a vigorous or passive way; and people user data could also be exploited in unauthorized ways that. As an example, a salesperson from a pharmacy may submit malicious matching queries to get statistics on patients' medications for promoting functions. To address user identification in MSNs, it's essential to disclose stripped-down and necessary personal data to as few users as attainable. In

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 148-151 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

fact, the perfect scenario is to let the instigator and its best matching user directly and in camera ascertain and connect to each alternative, while not knowing something regarding alternative users' profile attributes, whereas the remainder of the users ought to additionally learn nothing regarding the 2 user's matching attributes. However, it is difficult to search out the matching users in camera whereas efficiently. One might imagine of merely turning off the wireless telephone or input only a few attributes, however these would interfere with the system usability. Recently, Yang et. al. Proposed E-SmallTalker [2], a sensible system for matching people's interests before initiating a small-talk. However, E-SmallTalker suffers from the wordbook attack that doesn't totally defend the non-match attributes between 2 users. Another issue of private matching below a MSN setting is that the lack of a centralized authority. Lu et. al. [3] planned a proof matching theme for mobile health social networks, assuming the existence of a semi-online central authority. In this paper, we tend to overcome the higher than challenges and create the following main contributions.

(1) We tend to formulate the privacy preservation downside of profile matching in MSN. 2 levels of privacy area unit outlined in conjunction with their threat models, wherever the upper privacy level leaks less profile data to the soul than the lower level.

(2) We tend to propose 2 totally distributed privacy-preserving profile matching schemes, one in every of them being a non-public set intersection (PSI) protocol and also the alternative may be a personal cardinality of set-intersection (PCSI) protocol. However, solutions primarily based on existing PSI schemes area unit off from economical. We tend to leverage secure multi-party computation (SMC) supported polynomial secret sharing, and propose many key enhancements to improve the computation and communication potency. Also, users will select customized privacy levels once running the same matching instance.

(3) We offer formal security proofs and intensive performance evaluation for our schemes.Our 2 protocols area unit shown to be secure below the honest-but-curious (HBC) model, with information-theoretic security (for PSI) and commonplace security (for PCSI), severally. we tend to additionally discuss attainable extensions to stop malicious attacks. Meanwhile, they are shown to be a lot of economical than previous schemes that win similar security guarantees below the standard settings of MSN.

EXISTING SYSTEM:

In existing systems for such services, sometimes all the users directly publish their complete profiles for others to look. However, in several applications, the users' personal profiles could contain sensitive data that they are doing not wish to create public.

DISADVANTAGE:

- Opens up the likelihood for hackers to commit fraud and launch spam and virus attacks.
- Increases the danger of individuals falling prey to on-line scams that appear real, leading to knowledge or fraud.
- May end in negative comments from workers regarding the corporate or potential legal consequences if workers use these sites to look at objectionable, illicit or offensive material.
- Potentially leads to lost productivity, particularly if workers area unit busy change profiles.

PROPOSED SYSTEM:

In this paper, we have a tendency to overcome the on top of challenges and create the subsequent main contributions.

(1) We have a tendency to formulate the privacy preservation drawback of profile matching in MSN. 2 levels of privacy area unit outlined in conjunction with their threat models, wherever the upper privacy level leaks less profile info to the someone than the lower level.

(2) We have a tendency to propose 2 totally distributed privacy-preserving profile matching schemes, one among them being personal intersection protocol and also the alternative may be a private cardinality of set-intersection protocol. However, solutions supported existing PSI schemes area unit faraway from economical. We have a tendency to leverage secure multi-party computation supported polynomial secret sharing, and propose many key enhancements to boost the computation and communication potency.

ADVANTAGE:

- Proximity-based mobile social networking (PMSN) becomes increasingly common as a result of the explosive growth of good phones.
- Two reciprocally mistrusting parties, every holding a non-public knowledge set, collectively work out the intersection or the intersection cardinality of the 2 sets while not leaky any further info to either party.
- Facilitates open communication, resulting in increased info discovery and delivery.
- Allows staff to debate ideas, post news, raise queries and share links.
- Provides a chance to widen business contacts.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 148-151 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

- Targets a good audience, creating it a helpful and effective achievement tool.
- Improves business name and consumer base with bottom use of advertising.
- Expands research, implements selling campaigns, delivers communications and directs interested individuals to specific websites.

SYSTEM IMPLEMENTATION

SECURITY

Since the users may have different privacy requirements and it takes different amount of efforts to achieve them, we hereby (informally) define two levels of privacy where the higher level leaks less information to the adversaries.

USABILITY AND EFFICIENCY

For profile matching in MSN, it is desirable to involve as few human interactions as possible. In this paper, a human user only needs to explicitly participate in the end of the protocol run, e.g., decide whom to connect to based 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.*

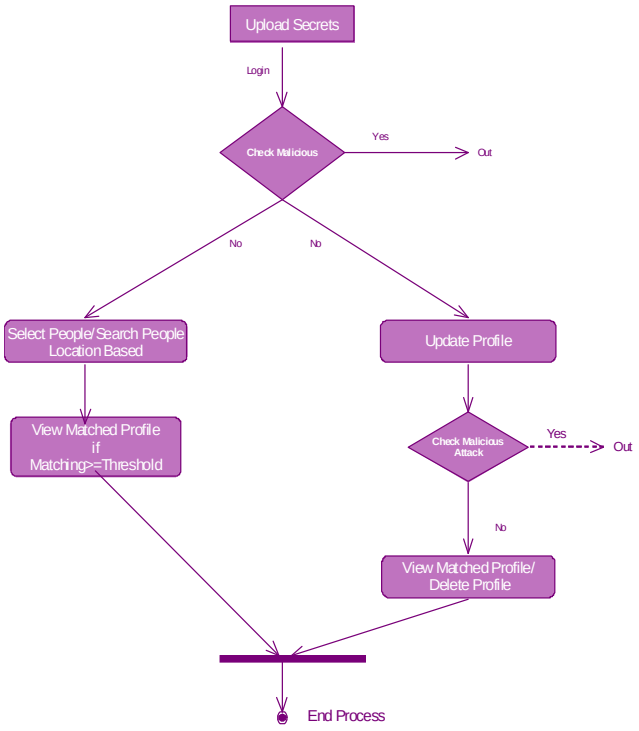
SHAMIR SECRET SHARING SCHEME

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.

PREVENTING MALICIOUS ATTACKS

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 "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'.

ARCHITECTURE



SIMULATION STUDY

METHODOLOGY: We implement our planned schemes and two previous schemes, FC10 and FNP, in NS-2 [29]. We simulate the protocols' communications and computations by telling the machine the sizes and variety of packets every party ought to send, fill every packet with dummy contents, and estimate the latency of every computation. Note that, in each round/step, we tend to exploit the opportunities to combination messages sent to an equivalent party into one packet the maximum amount as potential, so as to cut back the quantity of packets sent. Additionally, we only simulate one full protocol run, because the time variance is extremely small attributable to settled programming.

CONCLUSION:

In this paper, we tend to for the primary time formalize the matter of privacy-preserving distributed profile matching in MSNs, and propose 2 concrete schemes that win increasing levels of user privacy preservation. Towards planning light-weight protocols, we tend to utilize Shamir secret sharing because the main secure computation

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 148-151 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

technique, whereas we tend to propose further enhancements to lower the planned schemes' communication prices.

Through intensive security analysis and simulation study, we show that 1) our schemes square measure evidenced secure underneath the HBC model, and may be simply extended to stop sure active attacks; 2) our schemes square measure way more economical than state-of the art ones in MSNs wherever the network size is within the order of tens, and once the quantity of question attributes is smaller than the quantity of profile attributes.

REFERENCES

[1] M. Li, N. Cao, S. Yu, and W. Lou, "Findu: Privacy-preserving personal profile matching in mobile social networks," in *IEEEINFOCOM '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.
[13] S. Jarecki and X. Liu, "Efficient oblivious pseudorandom function with applications to adaptive ot and secure computation of set intersection," in *TCC '09*. Berlin, Heidelberg: Springer- Verlag, 2009, pp. 577–594.
[14] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in *IEEE INFOCOM '11*, Apr 2011, pp. 1–9.
[15] E. De Cristofaro, M. Manulis, and B. Poettering, "Private discovery of common social contacts," in *Applied Cryptography and Network Security*. Springer, 2011, pp. 147–165.
[16] 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, pp. 84 –92.
[17] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.
[18] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation."

AUTHORS

Himabindu Venigalla received the M.C.A degree in Computer Science & Engineering from Nagarjuna University, Guntur in 2011 & pursuing her M.Tech in Computer Science & Engineering from JNTU Kakinada.

Dr. P. Harini is presently working as a professor and HOD, Dept of Computer Science and Engineering ,in St.Ann's College of Engineering and Technology, Chirala. She obtained Ph.D in distributed and Mobile Computing from JNTUA, Ananthapur. She Guided Many UG and PG Students. She has More than 18Years of Excellence in Teaching and 2 Years of Industry Experience. She published more than 20 International Journals and 25 Research Oriented Papers in Various Areas. She was awarded **Certificate of Merit** by JNTUK, Kakinada on the University Formation Day on 21 - August - 2012.