ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Privacy Preserving Friending in Decentralized Mobile Social Networks

Aditya Waghmare [1], Ashish Kothawade[1], Prajakta Kakade[1] , Bhagyashri Markad[1], Prof. Mrs B. L. Dhote[2]

Student, Department of Computer Engineering, Sinhgad College of Engineering Lonavala, Savitribai Phule Pune University, India[1]

Student, Department of Computer Engineering, Sinhgad College of Engineering Lonavala, Savitribai Phule Pune University, India[2]

ABSTRACT-As the increasing use of mobile devices, mobile social networks (MSNs) are becoming an inseparable part of people's lives. In existing systems for such services, connection to the Internet and consequently using third-party services is a requisite. The paper explores a MSN system which doesn't require a third-party service and works on decentralized network, such as wireless tethering, Wi-Fi or Bluetooth.The system in its core is a profile matching application which helps user to find the people whose profile best matches with others people in a secure fashion. Also the possibility is explored to integrate a proximity-based and location based system.

KEYWORDS: Privacy preserving profile matching,secure communication, decentralized mobile social networks

I. INTRODUCTION

In the last few years, mobile hand-held devices in the market have exponentially increased and have pervaded almost everywhere. Thus it comes as no surprise that majority of social networking services are designed for mobile users. Existing Mobile Social services like WhatsApp, Viber, Hike etc require to be connected to the Internet and are essentially third-party services. The drawback of these systems are that many of the mobile users have problem in having connecting the internet because of expensive tariffs or mobile connectivity not available everywhere. Thus an effective solution is to develop a proximity-based decentralized mobile social service that works without connecting to the Internet and without using any kind of third-party services. The various methods of connection are short-range networks such as Wi-Fi and bluetooth. The obvious challenge in any Mobile Social Network(MSN) is to maintain privacy of users who share their profiles over the network. Also many users may not be comfortable in socializing with strangers near their vicinity.To mitigate these obvious challenges, one has to ensure secure communication over the network and proper profile matching using protocols such as private-set interesection(PSI) or private cardinality set of Intersection (PCSI) can be used. The drawback of conventional profile matching algorithms is that only one user gets to know whether the profile is matched or not. In existing systems, secure communication is usually obtained by using public-key cryptosystem. But this approach involves a trusted third-party system and requires key management, which may be difficult to achieve in a decentralized MSN.

II. LITERATURE SURVEY

E. De Cristofaro and G. Tsudik[1] explore some Private Set Intersection (PSI and APSI)variations and constructs several secure protocols that areappreciably more efficient than the state-of-the-art.The choice between PSI and APSI depends on whether one needs clientauthorization or server unlinkability, also server's ability to engage in pre-computation. Evaluation is performed to highlight the differences between existing PSI techniques and other protocols. The focus here is on performance in terms of server and client computationand communication complexities. The limitation is that tests and analysis of the protocols used are not done against malicious parties as well as in a group setting.[1]

DOI: 10.15680/IJIRCCE.2016. 0411142

W. Dong, V. Dave, L. Qiu, and Y. Zhang[2] proposenovel techniques and protocols to determine social proximitybetween two users to discover potential friends and proposes to develop a secure friend discovery protocol for mobile socialnetworks, and use both analysis and real implementation todemonstrate its feasibility and effectiveness. The protocols are tested on HP IPAQ 910, whichhas Marvell PXA270 416 MHz Processor, 128 MB RAM,Windows Mobile 6.1 Professional operating system, 802.11b/g WiFi cardand .NET Compact Framework. An essential capability offered by mobile social networks isto allow mobile users to discover and interact with friends whohappen to be in their physical vicinity. Limitations are that it creates seriousprivacy and security concerns,for example, people are oftenreluctant to reveal their presence and personal profile to anarbitrary person in their vicinity. Also the broadcast nature of wireless mediumalso makes it easy for a malicious user to spoof and inject traffic into the mobile social networks.[2]

Rui Zhang,Jinxue Zhang, Yanchao Zhang,Jinyuan Sun, Guanhua Yan[3] tackle the challenge of designing a Proximity-based Mobile Social Network(PMSN) by designing novel fine-grained private matchingprotocols that enable two users to perform profile matching without disclosing anyinformation about their profiles beyond the comparison result. The paper helps in formulating the problem of fine-grained private (profile) matching for proximity-based mobile socialnetworking and presents a suite of novel solutions thatsupport a variety of private-matching metrics at different privacy levels. The implementation of protocols is done on LG P-970smartphones, which has a 1GHz Cortex-A8 processor, 512 MBRAM, Android v2.2 Operating System, a 802.11 b/g/n WiFiinterface, and Bluetooth v2.1 with Enhanced Data Rate (EDR).A major challenge for profile matching is to ensure theprivacy of personal profiles which often contain highly sensitiveinformation related to gender, interests, political tendency,health conditions, and so on. The limitations are Manipulating protocol output, Repeatedly matching with different profiles and Denial-of-Service attack.[3]

IV. CONCLUSION

The paper has analyzed and surveyed various protocols and methodologies in existing mobile social network services. The conclusion derived in this paper is that having a competent secure communication channel such as Advanced Encyption System(AES) algorithm, data integrity done by SHA protocols and having a decentralized MSN containing key encryption based profile matching without doing any kind of preset or using any kind of third party service.

REFERENCES

[1] E. De Cristofaro and G. Tsudik, “Practical private set intersection protocols with linear complexity,” in Proc. 14th Int. Conf. Financial Cryptography Data Security, 2010.
[2] W. Dong, V. Dave, L. Qiu, and Y. Zhang, “Secure friend discovery in mobile social networks,” in Proc. IEEE INFOCOM, 2011.
[3] Rui Zhang, Member, IEEE, Jinxue Zhang, Yanchao Zhang, Senior Member, IEEE,Jinyuan Sun, Member, IEEE, and Guanhua Yan,“Privacy Preserving Profile Matching For Proximity Based Mobile Social Network”
[4] M. Chase, “Multi-authority attribute based encryption,” in Proc. 4th Conf. Theory Cryptography.
[5] M. J. Freedman, K. Nissim, and B. Pinkas, “Efficient private matching and set intersection,” in Proc. Int. Conf. Theory Appl. Cryptographic Tech.
[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. 13th ACM Conf. Comput. Commun. Security, 2006.
[7] Magnetu [Online]. Available: http://magnetu.com, 2013.
[8] Tencent weibo [Online]. Available: http://t.qq.com/, 2013.