International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Survey on Profile Privacy and Communication Security in Social Network

Vina M. Lomte[1], Harshal Bhosale[2]

[1]HOD, Computer Engineering Department, RMD Sinhgad School of Engineering, Savitribai Phule University, Pune, India

[2]ME student, Computer Engineering Department, RMD Sinhgad School of Engineering, Savitribai Phule University, Pune, India

Abstract: ***There are many social networks developed who serve connection between two or more people. Such social networks also help to find matching profiles within certain area. Using social networks for communication has some challenging task like protecting user information or profile. In this paper, a mechanisms has been discussed, in which user gives some preferences and the matching profile based on those preferences is searched in the distributed social network. The mechanism is to have secure communication channel between the requester and matching profiles at the time when a matching profile is found based on preferences given by requester. In this mechanism a secure communication is established so that the requester and matched profiles cannot cheat on each other or they cannot pretend to be matched. The extensive survey has concluded that such mechanisms are very effective and secure in social networks.***

Keywords: Privacy preserving profile matching, secure communication,

1. Introduction

A client in a MANET i.e. versatile impromptu long range interpersonal communication framework normally has his own particular a profile which contains an arrangement of properties. The trait can be anything produced by the framework or information by the client which incorporates clients area, places he/she has been to, social gatherings, encounters, intrigues, contacts and so forth. It has been watched that there are two surely understood long range interpersonal communication frameworks Facebook and Tencent Weibo, having more than 90 percent clients have interesting profiles. In this manner for most clients, the complete profile can be his/her unique mark in informal communities. The profile could be exceptionally helpful for looking and friending individuals. Yet, it is additionally exceptionally unsafe to uncover the unique mark to outsiders. At that point, in most interpersonal organizations, friending as a rule makes two regular strides: profile coordinating and correspondence.

2. Literature Review

2.1 Message in a Sealed Bottle: Privacy Preserving Friending in Social Networks.

Authors: Lan Zhang, Xiang-Yang Li

Numerous nearness based versatile interpersonal organizations are produced to associations between any two individuals, or to help a client to discover individuals with coordinated profile inside of a sure separation. A testing undertaking in these applications is to ensure the security the members' profiles and individual hobbies. Author outlines novel instruments, when given an inclination profile put together by a client, that hunt a man with coordinating profile in decentralized multi-bounce versatile interpersonal organizations. The systems are security protecting: no members' profile and the submitted inclination profile are uncovered. The systems set up a safe correspondence channel between the initiator and coordinating clients when the coordinating client is found.[1] The thorough examination demonstrates that the system is secure, protection safeguarding, obvious, and productive both in correspondence and calculation. Broad assessments utilizing genuine interpersonal organization information, and real framework execution on advanced cells demonstrate that the systems are essentially more effective than existing arrangements.

2.2 Improving Privacy and Security in Multi-Authority Attribute-Based Encryption

Authors: Melissa Chase, Sherman S.M. Chow

Trait based encryption (ABE) decides unscrambling capacity in view of a client's qualities. In a multi-power ABE plan, numerous trait powers screen distinctive arrangements of properties and issue comparing unscrambling keys to clients, and encryptors can require that a client acquire keys for fitting qualities from every power before decoding a message. Pursue gave a multi-power ABE plan utilizing the ideas of a trusted focal power (CA) and worldwide identifiers (GID). In any case, the CA in that development has the ability to unscramble each ciphertext, which appears to be by one means or another conflicting to the first objective of dispersing control over numerous possibly untrusted powers. Additionally, in that development, the utilization of a reliable

GID permitted the powers to join their data to construct a full profile with the greater part of a client's properties, which pointlessly bargains the client's protection.[2] Author proposes an answer which uproots the trusted focal power, and secures the clients' protection by keeping the powers from pooling their data on specific clients, along these lines making ABE more usable practically speaking.

2.3 Cipher text-Policy Attribute-Based Encryption
Authors: Bhoopathy, V., Parvathi, R.M.S.

In a few conveyed frameworks a client ought to just have the capacity to get to information if a client groups a sure arrangement of certifications or properties. As of now, the main strategy for upholding such approaches is to utilize a trusted server to store the information and intercede access control. Notwithstanding, if any server putting away the information is traded off, then the confidentiality of the information will be traded off. In this paper authors show a framework for acknowledging complex access control on scrambled information that we call Ciphertext-Policy Attribute-Based Encryption.[3] By utilizing the procedures encoded information can be kept confidential regardless of the possibility that the stockpiling server is untrusted; in addition, the routines are secure against agreement assaults. Past Attribute-Based Encryption frameworks utilized credits to portray the scrambled information and incorporated arrangements with client's keys; while in the framework credits are utilized to depict a client's qualifications, and a gathering encoding information decides an arrangement for who can unscramble. In this manner, the techniques are theoretically closer to customary access control systems, for example, Role-Based Access Control (RBAC). Furthermore, authors give an execution of the framework furthermore, give execution estimations.

2.4 Practical Private Set Intersection Protocols
Authors: Emiliano De Cristofaro and Gene Tsudik

The always expanding reliance on whenever anyplace accessibility of information and the comparably expanding apprehension of losing protection spur the requirement for security saving methods. One between besting and regular issue happens when two gatherings need to secretly figure a convergence of their particular arrangements of information. In doing as such, one then again both sides must get the crossing point (if one exists), while not one and the other should learn anything about other set components.[4] Albeit former work has yielded various effective and exquisite Private Set Intersection (PSI) methods, the mission for efficiency is still in progress. This paper investigates some PSI varieties and builds a few secure conventions that are appreciably more efficient than the cutting edge.

3. Proposed System

Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) are proposed by Goyalet al. and Bethencourtet al.[5] respectively to overcome the aforementioned drawback of fuzzy IBE. They look similar, but ciphertext and key structures are totally different, and the decision of encryption policy (who can or cannot decrypt the message) is made by different parties.

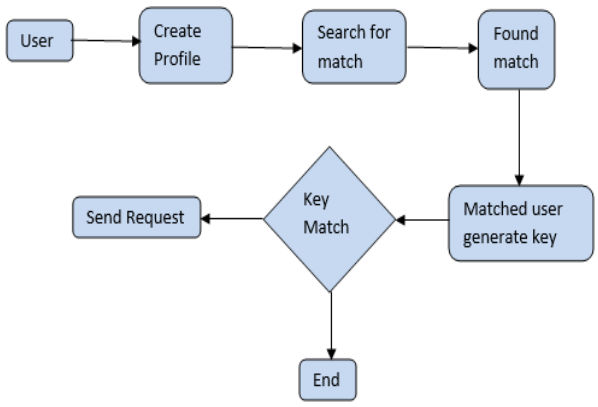

Figure: System architecture

3.1 Profile Vector and Key Generation

In this module is separate key is created which is the key of the required profile, the initiator scrambles the secret message utilizing a symmetric encryption procedure like Advanced Encryption Standard (AES). Any individual who gets it tries to decode the secret message with his/her own profile key. Just the precisely coordinating individual will decode the message accurately.

3.2 Remainder vector

A remainder vector are designed to significantly reduce the computation and communication overhead of unmatched users.

3.3 Hint Matrix

A hint matrix is constructed to support a flexible fuzzy search.

3.4 CP-ABE:
In the CP-ABE, the private key is distributed to users by a trusted central issuer only once. The keys are identified with a set of descriptive attributes, and the encrypter specifies encryption policy using an access tree so that those with private keys which satisfy it can decrypt the ciphertext.

4. Conclusion and Future Scope

In this paper, symmetric key encryption based protection safeguarding profile coordinating and secure correspondence divert foundation system in decentralized social network with no pre-setting or trusted outsider is discussed. A few conventions were proposed for accomplishing undeniable nature and diverse levels of protection. Authors led broad assessments on the exhibitions utilizing an expansive scale dataset from genuine person to person communication. The outcomes demonstrate that the instruments beat existing routines essentially and give productive and secure answer for versatile informal communities. The productive procedures, counting private fluffy characteristic coordinating and secure correspondence channel building up, can likewise be connected to numerous different situations where gatherings don't as a matter of course trust one another, e.g., promoting closeout, information sharing and

area based administrations. In future work, these methods can be incorporated into all the more systems networking frameworks.

References

[1] Lan Zhang , Kebin Liu , Taeho Jung and Yunhao Liu "Message in a Sealed Bottle: Privacy Preserving Friending in Mobile Social Networks" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 9, SEPTEMBER 2015.
[2] Melissa Chase and Sherman S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption"
[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute- based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.
[4] E. De Cristofaro and G. Tsudik, "Practical private set intersection protocols with linear complexity," in Proc. 14th Int. Conf. Financial Cryptography Data Security, 2010, pp. 143–159.
[5] Taeho Jung, Xiang-Yang, Zhiguo Wan, "Privacy Preserving Cloud Data Access With Multi-Authorities", 2013 Proceedings IEEE INFOCOM.

Author Profile

Prof. Vina M. Lomte is the HOD of Computer Dept. at RMD SSOE, Pune, having more than 10+ years of experience in the field of teaching and research. The domains of her research are Software Testing, Software Engineering and Web Security.

Mr. Harshal Bhosale is pursuing his Masters of Engineering in the Computer Engineering Department, Sinhgad School of Engineering, Savitribai Phule University Pune. He received Bachelor of Engineering degree in Information Technology from University of Pune, Maharashtra, India.