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 6, June 2016

Profile Privacy and Communication Security in Social Network

Harshal A. Bhosale, Prof. Vina M. Lomte

ME Student, Department of Computer Engineering, RMD Sinhgad SOE, Warje, Savitribai Phule Pune University, Maharashtra

HOD, Department of Computer Engineering, RMD Sinhgad SOE, Warje, Savitribai Phule Pune University, Maharashtra

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 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 focused 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

I. 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.

II. RELATED WORK

Lan Zhang[1] 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 between the initiator and coordinating clients when the coordinating client is found.[1] 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)[2] 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. Melissa Chase[2] 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. Bhoopathy[3] show a framework for

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 6, June 2016

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. Albeit former[4] work has yielded various effective and exquisite Private Set Intersection (PSI) methods, the mission for efficiency is still in progress.[4] This paper investigates some PSI varieties and builds a few secure conventions that are appreciably more efficient than the cutting edge.

III. 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.

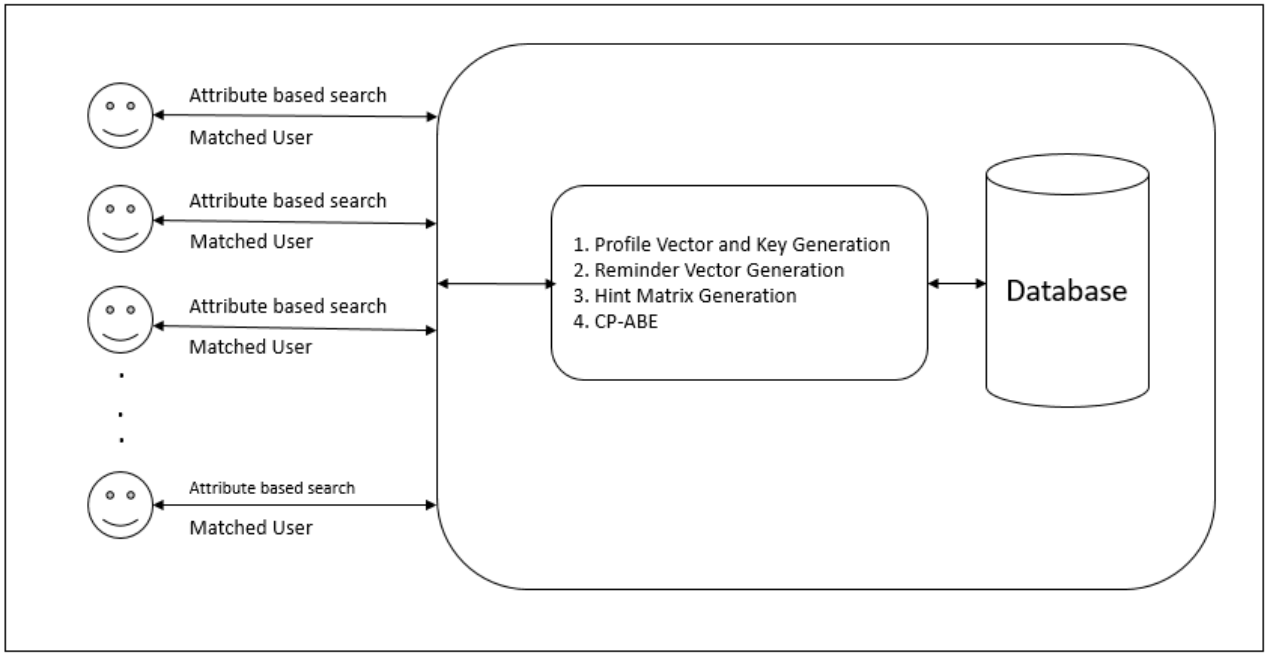

Fig: System Architecture

- **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.
  To protect the profile privacy and support a fuzzy search, a cryptographic hash (e.g. SHA-256) of the attribute is adopted as the attribute equivalence criterion in this mechanism.
  Assume the cryptographic hash function is H which yields n-bit length hash value. With a sorted normalized profile:

$$A_k = (a_k^1, a_k^2, a_k^3 \ldots a_k^m)$$

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 6, June 2016

$$H_k = H(A_k) = (h_k^1, h_k^2, h_k^3 \ldots h_k^m)$$
$$here h_k^i = H(a_k^i,)$$

A profile key generated with H_k is

$$K_k = H(H_k)$$

- **Reminder Vector:** A remainder vector are designed to significantly reduce the computation and communication overhead of unmatched users. A remainder vector consists of the remainders of all hashed attributes in the input H_k divided by *P*

$$R_k = (h_k^1 mod\ p, h_k^2 mod\ p, h_k^3 mod\ p \ldots h_k^m mod\ p)$$

- **Hint Matrix:** A hint matrix is constructed to support a flexible fuzzy search.

- **CP-ABE:** In CP-ABE, private key is distributed to users by system:

CP-ABE states:
Setup(*PK*)
Encrypt(*PK, M, A*)
Key Generation(*MK, S*)
Decrypt(*PK, CT, SK*)

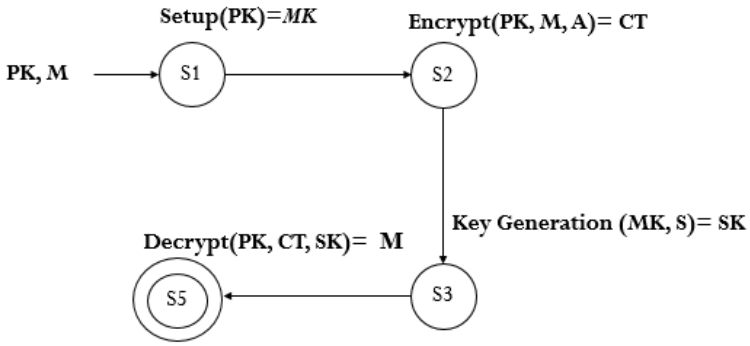

Fig: State Diagram

IV. SIMULATION RESULTS

The proposed system if efficient and secure in nature. Almost each and every attribute in the system is secured in order to make the user profile private. The profiles and the communication messages are secured at database level so that any intruder who gets access to database cannot disclose user's personal data. The reminder and hint matrix give us the result in shortest span of time.

Here are the examples:

Time in milliseconds	Reminder Matrix	Hint Matrix
Start Time	1466946110121	1466946136166
End Time	1466946110921	1466946139329
Execution Time	800	3163

Table: Execution Time

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 6, June 2016

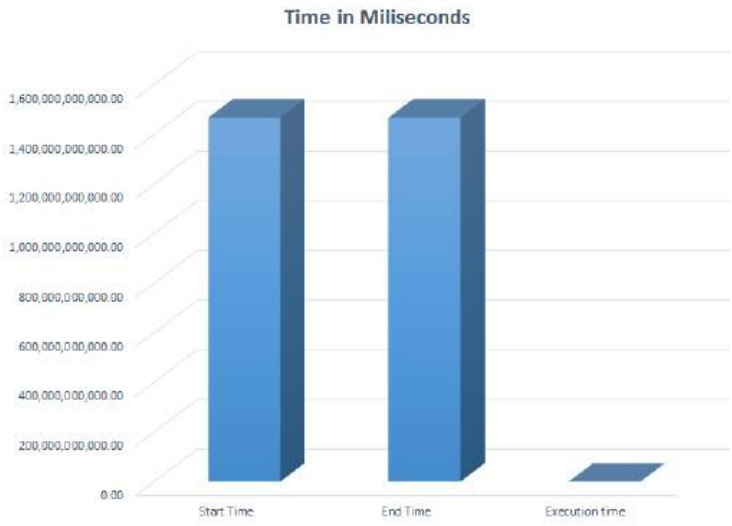

Fig: System Performance using Reminder and Hint Matrix

V. CONCLUSION AND FUTURE WORK

In the proposed system, 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 level of protection. We led broad assessment on the exhibitions utilizing an expensive scale dataset from genuine person to person communication. The outcome demonstrate that the instruments beat existing routes essentially and give productive and secure answer for versatile informal communities. The productive procedures, counting private fluffy characteristics 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.As the current security mechanism is only focused on social network database security, future work can be carried out to secure communication channel between two users in the network.

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. 321334.
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. 143159.
5. Taeho Jung, Xiang-Yang, Zhiguo Wan, "Privacy Preserving Cloud Data Access With Multi-Authorities", 2013 Proceedings IEEE INFOCOM.
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, pp. 8998.
7. I. Ioannidis, A. Grama, and M. Atallah, "A secure protocol for computing dot-products in clustered and distributed environment in Proc." IEEE Int. Conf. Parallel Process., 2002, p. 379.
8. T. Jung, X. Mao, X.-Y. Li, S. Tang, W. Gong, and L. Zhang, Privacy-preserving data aggregation without secure channel: multivariate polynomial evaluation, in Proc. IEEE INFOCOM, 2013, pp. 26342642.

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 6, June 2016

BIOGRAPHY

Mr. Harshal A. Bhosale received B.E. degree in Information Technology in the year 2013 from Smt. Kashibai Navale College of Engineering, Pune and pursuing M.E. in Computer Engineering from RMD SSOE,Warje, Pune.

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