Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 6, June -2017

Attribute-Based Secure Friend Discovery in Online Social Networks

[1]Kirti Bodkhe,[2]Prof. Archana Lomte

[1]*ME.Student,Computer Department, JSPM's Bhivarabai Sawant Institute of Technology & Research,Pune.*
[2]*Prof,Computer Department, JSPM's Bhivarabai Sawant Institute of Technology & Research,Pune.*

Abstract — *Many proximity-based mobile social networks are developed to facilitate connections between any 2 folks, or to assist a user to seek out folks with a matched profile at intervals an exact distance. A difficult task in these applications is to guard the privacy of the participants' profiles and communications. during this paper, we have a tendency to style novel mechanisms, once given a preference-profile submitted by a user that search persons with matching-profile in redistributed mobile social networks. Meanwhile, our mechanisms establish a secure line between the leader and matching users at the time once an identical user is found. These techniques may be applied to conduct privacy conserving keywords based mostly search with none secure line. Our analysis shows that our mechanism is privacy-preserving (no participants' profile and therefore the submitted preference-profile are exposed), verifiable (both the leader and any unmatched user cannot cheat one another to faux to be matched), and economical in each communication and computation. In-depth evaluations exploitation real social network information and actual system implementation on sensible phones show that our mechanisms are considerably additional economical than existing solutions. As a contribution we have a tendency to present an anonymous privilege management theme Annoy Control to deal with not only the info privacy drawback in Server storage, however additionally the user identity privacy problems in existing access management schemes. By exploitation multiple authorities in Server ADP system, our projected theme achieves anonymous Server information access and fine grained privilege management. Our security proof and performance analysis shows that Annoy Control is each secure and economical for Server computing atmosphere.*

Keywords- *Reminder Matrix, Hint Matrix, Attribute-Based Encryption.*

I. INTRODUCTION

Friending and communication are two essential fundamental functions of social networks. When individual people join social networks, they generally get started by generating a profile, and then interact with other end users. The content material of profile could be extremely broad, this kind of as personalized background, hobbies, contacts, and locations they have been to, and so on. Profile matching is a frequent and beneficial way to make new buddies with mutual interests or experiences, locate misplaced connections or search for specialists [30].

Consumers in a MANET i.e. mobile ad hoc social networking technique generally have his personal a profile which includes a set of attributes. The attribute can be anything at all created by the technique or input by the consumer which consists of consumer's place, locations he/she has been to, pastime, occupation, social groups, experiences, interests, contacts and so on. It has been observed that there are two effectively identified social networking techniques Facebook and Tencent Weibo, obtaining much more than 90% end users have exclusive profiles. Hence for most end users, the full profile can be his/her fingerprint in social networks. The profile could be extremely beneficial for browsing| and friending individual people but it is also really risky to reveal the fingerprint to strangers. Then, in most social networks, friending generally requires two common methods: profile matching and communication [1] [5]. These applications lead to a variety of privacy issues. A safe communication channel is equally essential but frequently ignored in OSN. Dealing with these issues, the technique very first formally defines the privacy preserving verifiable profile matching difficulty in decentralized social network. We then propose protocols to deal with the privacy preserving profile matching and safe communication channel establishment in decentralized social networks without having any presetting or trusted third get together. We consider benefit of the frequent attributes in between matching end users, and use it to encrypt a message with a secret channel important in it. In our mechanisms, only a matching consumer can decrypt the message. A privacy-preserving profile matching and safe channel development are finished concurrently with only a one particular} round of communication with technique. The safe channel development resists the man-in-the-middle (MITM) assault by any unmatched end users. A sequence of effectively-developed schemes can make our protocols useful, versatile and light-weight, e.g., a remainder vector is developed to considerably minimize the computation and communication overhead of unmatched end users. Our profile matching mechanisms are also verifiable which thwart cheating about matching outcome. We also design and style a mechanism for place privacy preserved vicinity search primarily based on our fundamental scheme. In contrast to most current functions which are relying on the asymmetric cryptosystem and trusted- third-party, our protocols need no presetting and a lot much less computation. Our techniques can also be utilized to perform effective privacy preserving keywords and phrases primarily based search without having any safe communication channel, e.g., personal picture search and sharing.

The ever growing use of OSNs has launched a new paradigm in interacting with current buddies and creating new buddies in the on-line planet as effectively as in actual daily life. Recent personal profile matching schemes lead to privacy breaches. How to allow individual people to check out new buddies in OSNs although preserving their privacy is an essential and difficult issue. In this function, we have exploited the neighborhood construction of an OSN to define a reasonable asymmetric social proximity measure, and presented two effective protocols for privately computing the social proximity in between two end users in OSN.

II. LITERATURE SURVEY

1) Message in a Sealed Bottle: Privacy Preserving Friending in Social Networks.
Author: Lan Zhang_, Xiang-Yang Li†
Abstract:
Many proximity-based mobile social networks area unit developed to facilitate connections between any 2 folks, or to assist a user to seek out folks with matched profile among a particular distance. A difficult task in these applications is to guard the privacy the participants' profiles and private interests. during this paper, we have a tendency to style novel mechanisms, once given a preference-profile submitted by a user, that search an individual with matching-profile in redistributed multi-hop mobile social networks. Our mechanisms area unit privacy-preserving: no participants' profile and therefore the submitted preference-profile area unit exposed. Our mechanisms establish a secure line between the instigator and matching users at the time once the matching user is found. Our rigorous analysis shows that our mechanism is secure, privacy-preserving, verifiable, and economical each in communication and computation. in depth evaluations exploitation real social network information, and actual system implementation on sensible phones show that our mechanisms area unit considerably a lot of economical then existing solutions.
2) Joint Social and Content Recommendation for User-Generated Videos in Online Social Network
Author:Zhi Wang, *Student Member, IEEE,* Lifeng Sun, *Member.*
Abstract:
Online social network is rising as a promising different for users to directly access video contents. By permitting users to import videos and re-share them through the social connections, an oversized variety of videos area unit obtainable to users in the on-line social network. The ascension of the user generated videos provides monumental potential for users to seek out those that interest them; whereas the convergence of on-line social network service and on-line video sharing service makes it potential to perform recommendation victimization social factors and content factors put together. During this paper, we tend to style a joint social-content recommendation framework to counsel users that videos to import or re-share within the on-line social network. During this framework, we tend to 1st propose a user-content matrix update approach that updates and fills in cold user-video entries to produce the foundations for the advice. Then, supported the updated user-content matrix, we tend to construct a joint social-content house to live the connectedness between users and videos, which might offer a high accuracy for video mercantilism and re-sharing recommendation. We tend to conduct experiments victimization real traces from Tencent Weibo and Youku to verify our formula and assess its performance. The results demonstrate the effectiveness of our approach and show that our approach will well improve the advice accuracy.
3) Ciphertext-Policy Attribute-Based Encryption
Author: Bhoopathy, V., Parvathi, R.M.S.
Abstract:
In many distributed systems a user ought to solely be able to access information if a user posse a definite set of credentials or attributes. Currently, the sole technique forenforcing such policies is to use a sure server to store the info and mediate access management. However, if any server storing the info is compromised, then the confidentiality of the info is compromised. During this paper we have a tendency to gift a system for realizing complicated access management on encrypted information that we have a tendency to decision Cipher text-Policy Attribute-Based encoding. By exploitation our techniques encrypted information will be unbroken confidential notwithstanding the storage server is un-trusted; furthermore, our strategies area unit secure against collusion attacks. Previous Attribute- based mostly encoding systems used attributes to explain the encrypted information and designed policies into user's keys; while in our system attributes area unit accustomed describe a user's credentials, and a celebration encrypting information determines a policy for World Health Organization will decode. Thus, our strategiesare conceptually nearer to ancient access management strategies like Role-Based Access management (RBAC). Additionally, we offer an implementation of our systemand give performance measurements.
4)Improving Privacy and Security in Multi-Authority Attribute-Based Encryption
Author: Melissa Chase, Sherman S.M. Chow
Abstract:
Attribute primarily based encoding (ABE) [13] determines decipherment ability supported a user's attributes. in a very multi-authority ABE theme, multiple attribute-authorities monitor completely different sets of attributes and issue corresponding decipherment keys thereto users, and encryptions will need to get keys by user for applicable attributes from every authority before decrypting a message. Chase gave a multi-authority ABE theme exploitation the ideas of a trusty central authority (CA) and international identifiers (GID). However, the CA therein construction has the ability to decipher each ciphertext that looks somehow contradictory to the initial goal of distributing management over several probably un-trusted authorities. Moreover, therein construction, the employment of a uniform GID allowed the authorities to mix their info to make a full profile with all of a user's attributes that unnecessarily compromises the

privacy of the user. In this, they propose an answer that removes the trusty central authority, and protects the users' confidentiality by preventing the authorities from pooling their info on specific users, so creating ABE additional usable in observe.

5) Practical Private Set Intersection Protocols
Author:Emiliano De Cristofaro and Gene Tsudik
Abstract:

The perpetually increasing dependence on anytime-anywhere availableness of information and also the commensurately increasing concern of losing privacy inspire the requirement for privacy-preserving techniques. One interesting and customary drawback happens once 2 parties have to be compelled to in private reason AN intersection of their several sets of information. In doing therefore, one for each party should get the intersection (if one exists), whereas neither should learn something regarding alternative set components. Though previous work has yielded variety of effective and chic personal Set Intersection (PSI) techniques, the hunt for efficiency continues to be current. This paper explores some PSI variations and constructs many secure protocols that square measure appreciably a lot of efficient than the progressive.

III.PROPOSED SYSTEM

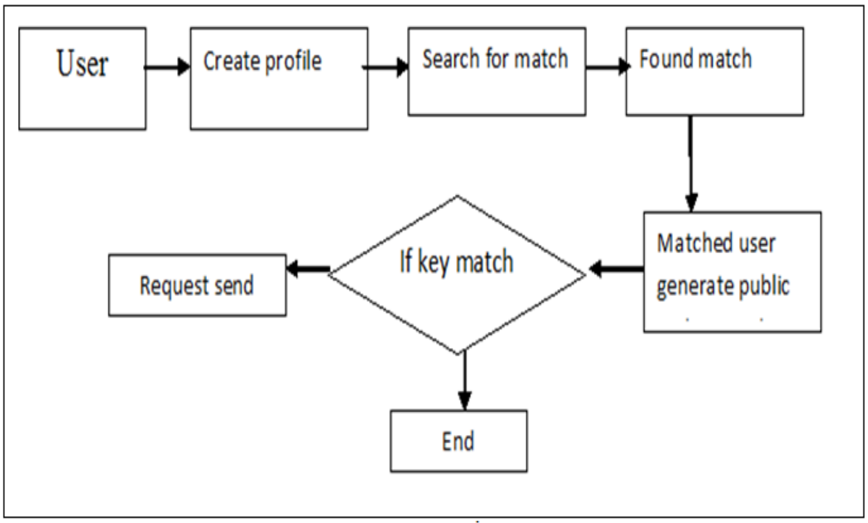


Fig.1 System Architecture

In proposed we design and style novel mechanisms, when provided a preference-profile submitted by a consumer, that search individual persons with matching-profile in on-line social networks. Meanwhile, our mechanisms create a safe communication channel in between the initiator and matching end users at the time when a matching consumer is identified. These methods can also be utilized to perform privacy preserving search phrases primarily based search without having any safe communication channel. Our evaluation demonstrates that our mechanism is privacy-preserving (no applicants' profile and the submitted preference-profile are showing), verifiable (together the initiator and any unmatched consumer can't cheat every other to pretend to be matched), and effective in each communication and computation.

At initial the initiator i.e. consumer will begins the procedure by making a request profile with the support of reminder matrix and hint matrix attribute and a secret message containing a channel key which is important for him/her. The initiator packs the encrypted message, the remainder vector and the hint matrix into a request bundle and sends it out. The request profile is a set of sorted attributes by each reminder and hint matrix attributes. Then he/she encrypts the attributes of the request profile a single by one particular to make a request profile vector. A profile is important created primarily based on the request profile vector making use of some publicly recognized hashing perform by submitted attributes. A remainder vector of the profile vector is yield for quick exclusion by a huge portion of unmatched individual persons. To help a versatile search requiring no excellent match, the initiator can define the required attributes, optional attributes and the similarity threshold of the matching profile. And a hint matrix is constructed from the request profile vector in accordance to the similarity definition, which allows the matching individual person to get the profiles important key to matched end users.

When a relay consumer receives a request from an additional consumer, he/she initial processes a quick check out of his/her personal profile vector with the remainder vector. If no sub-vector of his/ her profile vector fits the remainder vector, he/she is aware of that he/she is unmatched and will forward the request to other relay end users quickly. Otherwise, he/she is a candidate target and will produce a candidate profile vector set by some linear computation with his/her profile and the hint matrix. Then a candidate profile key is important to obtained set. In the fundamental mechanism, if any of his/her candidate keys can decrypt the message appropriately; he/she is a matching user and the browsing and secret important key exchange totally. Otherwise, he/she just forwards the request to other relay end users.

This procedure will continues until consumer or initiator will get relayed end users primarily based on reminder and hint matrix attributes.

IV.MATHEMATICAL MODEL

Let S is the Whole System Consists:

S = {U, m, P, RM, HM, SP}
Where,

1. ‘U’ is the set of users
   U = {u1, u2 . . . . un}.

2. ‘m’ is message to be sealed and sent.

3. ‘P’ is the set of created profile of U.

   P = {P1, P2 . . . Pn}.

4. ‘RM’ is the set of reminder matrix submitted by U.

   RM = {Urm1, Urm2 . . . Urmn}.

5. ‘HM’ is the set of hint matrix submitted by U.

   HM = {Uhm1, Uhm2 . . . Uhmn}.

6. ‘SP’ be the set of searched user profiles matched for U after search with RM and HM.

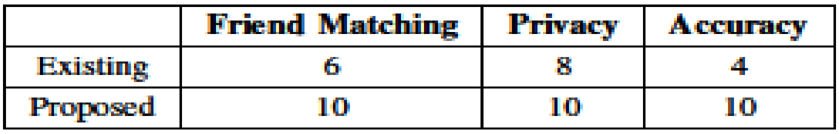
   S = {S1, S2 … Sn}.

Benefits of Proposed System:
1. Provide higher protection to consumer profile.
2. Introduced a remainder vector of the profile vector is yield for quick exclusion by a huge portion of unmatched individual person.
3. Privacy preservation of consumer information i.e. communication in between two end users.

Application:
The technique can utilized in on-line social networking websites sites exactly where consumer has no believe in on methods random suggestions and in which end users get matching profiles primarily based on their attributes.
Algorithm: AES-256
Implementing AES encryption algorithm for encryption of consumer search data i.e. reminder matrix information and hind matrix information and also communication i.e. messages in between two end users.

Result Analysis:

Input:
Here, Entire Technique taken numerous much more attribute for the input function but right here writer mostly focuses on the Time and efficiency of technique primarily based on this attributes we obtaining following outcome for our proposed technique.



	Friend Matching	Privacy	Accuracy
Existing	6	8	4
Proposed	10	10	10

Expected Result:

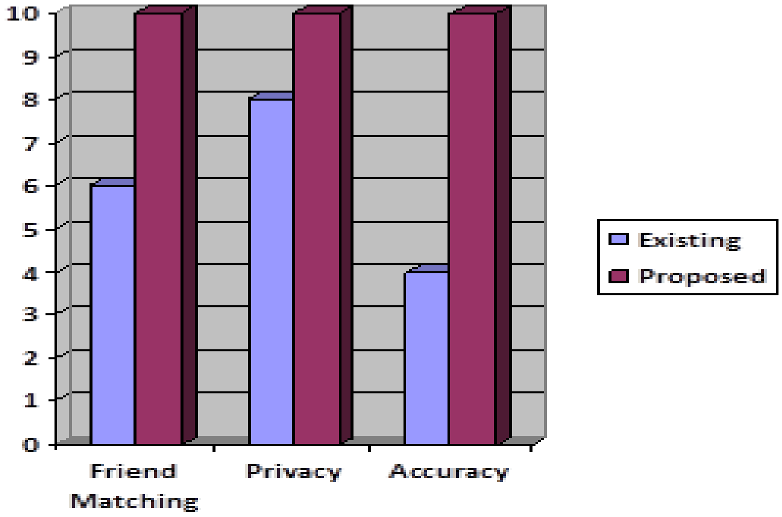


fig. 2 Expected Result Analysis

VI. CONCLUSION

The final results present that our mechanisms outperform current techniques considerably and give effective and safe answer for on-line social networks with attribute primarily based profile matching a recommendation. Our effective methods, which includes personal attribute matching and safe communication channel establishing, can also be utilized to numerous other situations in which events do not always believe in each and every other, e.g., marketing auction, details sharing and area primarily based on providers. In our long term function, we will integrate these methods into much more networking techniques.

ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the college powers for giving the obliged base and backing.

REFRENCES

[1] Magnetu [Online]. Available: http://magnetu.com, 2013.

[2] Tencent weibo [Online]. Available: http://t.qq.com/, 2013.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Security Privacy, 2007,pp. 321–334.

[4] M. Chase, "Multi-authority attribute based encryption," in Proc. 4th Conf. Theory Cryptography, 2007, pp. 515–534.

[5] E. De Cristofaro and G. Tsudik, "Practical private set intersection protocols with linear complexity," in Proc. 14th Int. Conf. FinancialCryptography Data Security, 2010, pp. 143–159.

[6] T. Jung, X.-Y. Li, Z. Wan, and M. Wan, "Control cloud data access privilege and anonymity with fully anonymous attribute based encryption," IEEE Trans. Inf. Forensics Security, 2015.

[7] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in Proc. IEEE INFOCOM, 2011,pp. 1647–1655.

[8] L. Zhang, X. Ding, Z. Wan, M. Gu, and X.-Y. Li, "Wiface: A secure geosocial networking system using wifi-based multi-hop manet," in Proc. 1st ACM Workshop Mobile Cloud Comput. Services: SocialNet. Beyond, 2010, p. 3.

[9] L. Zhang, T. Jung, P. Feng, X.-Y. Li, and Y. Liu, "Cloud-based privacy preserving image storage, sharing and search," arXiv preprintarXiv:1410.6593, 2014.

[10] M. J. Freedman, K. Nissim, and B. Pinkas, "Efficient private matching and set intersection," in Proc. Int. Conf. Theory Appl.Cryptographic Techn., 2004, pp. 1–19.

[11] 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. 89–98.

[12] B. Han and T. Baldwin, "Lexical normalisation of short text messages: Makn sens a# twitter," in Proc. 49th Annu. Meet. Assoc. Comput.Linguistics: Human Language Technol., 2011, vol. 1, pp. 368–378.