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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

A Survey on Message in a Sealed Bottle: Privacy Preserving Friending in Mobile Social Networks

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

ME.Student, Department of Computer Engineering, JSPM's Bhivarabai Sawant Institute of Technology & Research, Pune. Maharashtra, India

Professor, Department of Computer Engineering, JSPM's Bhivarabai Sawant Institute of Technology & Research, Pune .Maharashtra, India

ABSTRACT: Many proximity-based mobile social networks are developed to facilitate connections between any 2 folks, or to assist auser 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 presentan anonymous privilege management theme AnonyControl to deal with notonly 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 AnonyControl is each secure and economical for Server computing atmosphere.

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

I. INTRODUCTION

A user in a very Eduard Manet i.e. mobile unintentional social networking system sometimes has his own a profile that contains a group of attributes. The attribute will be something generated by the system or input by the user which incorporates user's location, places he/she has been to, social teams, experiences, interests, contacts etc. it's been determined that there square measure 2 accepted social networking systems Facebook and TencentWeibo, having quite ninety percent users have distinctive profiles. Therefore for many users, the entire profile will be his/her fingerprint in social networks. The profile might be terribly helpful for looking out and friending folks. However it's additionally terribly risky to reveal the fingerprint to strangers. Then, in most social networks, friending sometimes takes 2 typical steps: profile matching and communication. These applications cause variety of privacy considerations.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

II. LITERATURE SURVAY

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 TencentWeibo 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.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

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.EXISTING SYSTEM

In this paper, it style novel mechanisms, once given a preference-profile submitted by a user, that search an individual with matching-profile in suburbanised 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. Intensive evaluations using real social network knowledge, and actual system implementation on smart phones show that our mechanisms area unit considerably more efficient then existing solutions.

Disadvantages of Existing System:
1) Less security to user data.
2) Time consuming.

IV.PROPOSED SYSTEM

In 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 primarily based search with none secure line. Our analysis shows that our mechanism is privacy-preserving (no participants' profile and therefore the submitted preference-profile square measure exposed), verifiable (both the leader and any unmatched user cannot cheat one another to fake to be matched), and economical in each communication and computation. In depth evaluations mistreatment real social

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

network knowledge and actual system implementation on good phones show that our mechanisms square measure considerably additional economical than existing solutions.

Contribution:

We area unit coming up with and implementing a unique system of 2 on-line social networks that area unit connected to every other's to urge the notifications from one OSN to a different OSN. during this system user are registered to those OSN's by suggests that of a same email or username to the system in order that, suppose in OSN2 one user can post to one thing on his wall he can get notifications to a different OSN1 and regarding notification of latest friend request etc. and same with OSN2 to OSN1. There's no such existing system which can offers notifications from one OSN to OSN although an equivalent user exploitation that.

Advantages of Proposed System:

1) Provide high security to user profile.
2) Fast speed.
3) Privacy preservation of user knowledge.

V. MATHEMATICAL MODEL

1. Proposed system

Let S is the Whole System Consists:

S = {P, S, PR, PS, BA, R}.

1. P is the set of created profile.
   P= {P1, P2… Pn}
2. S is the set of search for match.
   S= {S1, S2, …Sn}.
3. PR is set of protection

PR= {PR1, PR2….PRn}.

4. PS is set of protection scheme sharing.
   PS= {PS1, PS2… PSn}.
5. BA is set block malicious user with message.
   BA= {BA1.BA2….BAn}.

Step 1: multiple user user create profile

P= {P1, P2…Pn}.

Step 2: Then it search for match .If match is found then it provide a protection else search for another.

S= {S1, S2,…Sn}.

Step 4: If search is found then protection is provided.

PR= {PR1, PR2….PRn}.

Step 5: Then private scheme sharing is applied.

PS= {PS1, PS2…PSn}.

Step 6: Then malicious message is blocked user.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

BA= {BA1, BA2….BAn}.

Output: Message is sent to correct matching user securely

2. Contribution:

Let W be the whole system which consist,

W = {U, OSN1, OSN2, P, S, N}

Where,

- U be the set of user.
  U = {U1, U2 . . . . Un}

- OSN1 & OSN2 be the two OSN's sites.

- P be the set of profiles created by U.
  P = {P1, P2 . . . . Pn}

- S is the set of status posted by U on particular OSN.

- N be the set of notification generated by particular user on OSN.

Step1 : At first user U will create a profile P on particular OSN1 with some unique username or id, then the same user U will also create the another profile on another OSN2 with unique username or id and it will provide the username of OSN1 by which the two OSN's will connect for particular user U.

Step2 : Suppose user U will post status S on OSN1 then he will get notification on his another profile which on OSN2 as well as on his email id, and also if he gets friend request from another user then also he will notified on his another OSN and vice a versa.

Output: Notifications form one OSN to another OSN.

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

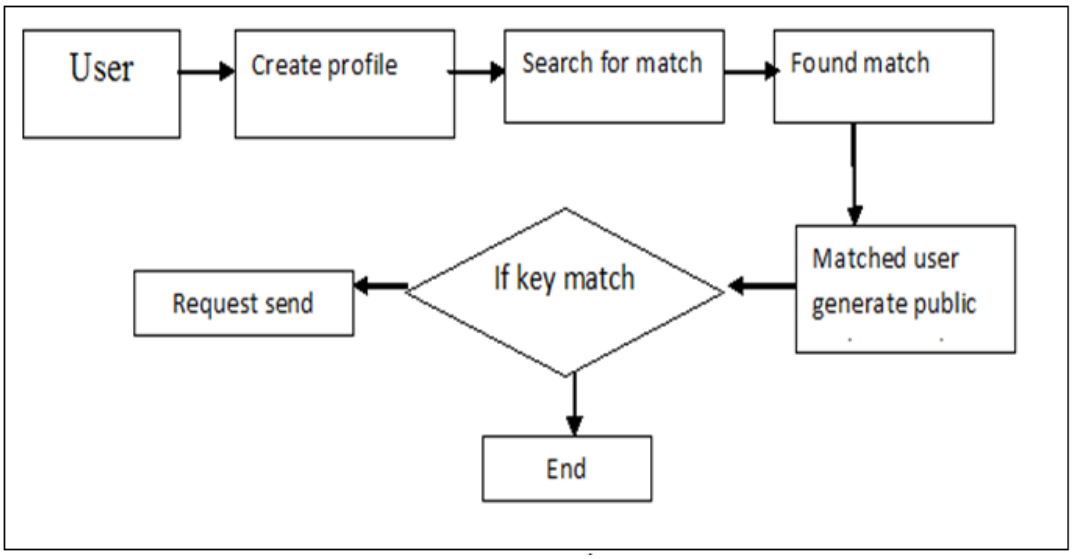
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

VI. SYSTEM ARCHITECTURE



VII. CONCLUSION AND FUTURE WORK

The ever increasing use of OSNs has introduced a brand new paradigmin interacting with existing friends and creating new friends within the on-line world still as in reality. Current privateprofile matching schemes cause privacy breaches. Howto modify individuals to explore new friends in OSNs whereas preservingtheir privacy is a vital and difficult downside.In this work,we have exploited the community structureof associate degree OSN to outline a practical uneven social proximitymeasure, and conferred 2 economical protocols for privatelycomputing the social proximity between 2 users in OSN.

REFERENCES

[1] Magnetu [Online]. Available: http://magnetu.com, 2013.
[2] Tencentweibo [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: Maknsens a# twitter," in Proc. 49th Annu. Meet. Assoc. Comput.Linguistics: Human Language Technol., 2011, vol. 1, pp. 368–378.