2581-4575

International Journal For Recent Developments in Science & Technology

Crossref

A Peer Reviewed Research Journal

SURVEY ON ASYMMETRIC SOCIAL PROXIMITY BASED PRIVATE MATCHING PROTOCOLS FOR ONLINE SOCIAL NETWORKS

[1]MR M SURESH, [2]DR ARVIND KUMAR RAI

[1]Assistant Professor, Dept of Computer science and engineering, Pullareddy Institute of Technology

[2]Professor, Dept of Computer science and engineering

University of Allahabad

Abstract — The explosive growth of on-line Social Networks (OSNs) over the past few years has redefined the approach folks act with existing friends and particularly create new friends. Some works propose to let folks become friends if they need similar profile attributes. However, profile matching involves Associate inherent privacy risk of exposing non-public profile info to strangers within the computer network. the prevailing solutions to the matter commit to shield users' privacy by in camera computing the intersection or intersection cardinality of the profile attribute sets of 2 users.These schemes have some limitations and may still reveal users' privacy. during this paper, we have a tendency to leverage community structures to redefine the OSN model and propose a sensible uneven social proximity live between 2 users. Then, supported the projected uneven social proximity, we have a tendency to style 3 non-public matching protocols, which give totally different privacy levels and may shield users' privacy higher than the previous works. we have a tendency to additionally analyze the computation and communication price of those protocols. Finally, we have a tendency to validate our projected uneven proximity live victimisation real social network information and conduct in depth simulations to guage the performance of the projected protocols in terms of computation price, communication price, total time period, and energy consumption. The results show the effectualness of our projected proximity live and higher performance of our protocols over the progressive protocols.

Keywords- On-line Social Networks (OSNs), Asymmetric social proximity, MANET, Mobile Social Networks (MSN), Private matching protocols.

I.INTRODUCTION

A user in a Manet i.e. mobile circumstantial social networking system typically has his own a profile that contains a collection of attributes. The attribute will be something generated by the system or input by the user which incorporates users location, places he/she has been to, social teams, experiences, interests, contacts etc. it's been ascertained that there area unit 2 accepted social networking systems Facebook and Tencent Weibo, having over ninety % users have distinctive profiles. so for many users, the whole profile will be his/her fingerprint in social networks. The profile can be terribly helpful for looking and friending folks. however it's conjointly terribly risky to reveal the fingerprint to strangers. Then, in most social networks, friending typically

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal


takes 2 typical steps: profile matching and communication. These applications cause variety of privacy issues.

II.LITERATURE SURVEY

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

AUTHORS: Lan Zhang_, Xiang-Yang Li

Many proximity-based mobile social networks square measure developed to facilitate connections between any 2 folks, or to assist a user to seek out folks with matched profile among an exact distance. A difficult task in these applications is to safeguard 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 someone with matching-profile in localized multi-hop mobile social networks. Our mechanisms square measure privacy-preserving: no participants' profile and therefore the submitted preference-profile square measure exposed. Our mechanisms establish a secure channel 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 mistreatment real social network information, and actual system implementation on good phones show that our mechanisms square measure considerably additional economical then existing solutions.

2.Joint Social and Content Recommendation for User-Generated Videos in Online Social Network

AUTHORS: Zhi Wang, Student Member, IEEE, Lifeng Sun, Member.

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 outsized variety of videos ar on the market to users in the on-line social network. The rapid climb 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 doable to perform recommendation victimization social factors and content factors put together. during this paper, we have a tendency to style a joint social-content recommendation framework to recommend users that videos to import or re-share within the on-line social network. during this framework, we have a tendency 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 have a tendency to construct a joint social-content area to live the relevancy between users and videos, which might give a high accuracy for video importation and re-sharing recommendation. we have a tendency to conduct experiments victimization real traces from Tencent Weibo and Youku to verify our rule and

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal


measure its performance. The results demonstrate the effectiveness of our approach and show that our approach will considerably improve the advice accuracy.

3.Ciphertext-Policy Attribute-Based Encryption

AUTHORS: Bhoopathy, V., Parvathi, R.M.S.:

In many distributed systems a user ought to solely be ready to access information if a user posses a precise set of credentials or attributes. Currently, the sole methodology for implementing such policies is to use a trusty server to store the info and mediate access management. However, if any server storing the info is compromised, then the con_dentiality of the info are going to be compromised. during this paper we tend to gift a system for realizing advanced access management on encrypted information that we tend to decision Ciphertext-Policy Attribute-Based coding. By victimisation our techniques encrypted information are often unbroken con_dential albeit the storage server is untrusted; furthermore, our ways ar secure against collusion attacks. Previous Attribute- primarily based coding systems used attributes to explain the encrypted information and engineered policies into user's keys; whereas in our system attributes ar accustomed describe a user's credentials, and a celebration encrypting information determines a policy for United Nations agency will decode. Thus, our ways ar conceptually nearer to ancient access management ways like Role-Based Access management (RBAC). additionally, we offer Associate in Nursing implementation of our system and provides performance measurements.

4.Improving Privacy and Security in Multi-Authority Attribute-Based Encryption AUTHORS: Melissa Chase, Sherman S.M. Chow

Attribute primarily based cryptography (ABE) [13] determines cryptography ability supported a user's attributes. in an exceedingly multi-authority ABE theme, multiple attribute-authorities monitor totally different sets of attributes and issue corresponding cryptography keys to users, and encryptors will need that a user acquire keys for acceptable attributes from every authority before decrypting a message. Chase gave a multi-authority ABE theme mistreatment the ideas of a sure central authority (CA) and world identifiers (GID). However, the CA in this construction has the ability to decipher each ciphertext, that appears somehow contradictory to the initial goal of distributing management over several probably untrusted authorities. Moreover, in this construction, the employment of the same GID allowed the authorities to mix their data to create a full profile with all of a user's attributes, that unnecessarily compromises the privacy of the user. during this paper, we have a tendency to propose an answer that removes the sure central authority, and protects the users' privacy by preventing the authorities from pooling their data on explicit users, therefore creating ABE a lot of usable in follow.

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

5.Practical Private Set Intersection Protocols

AUTHORS: Emiliano De Cristofaro and Gene Tsudik

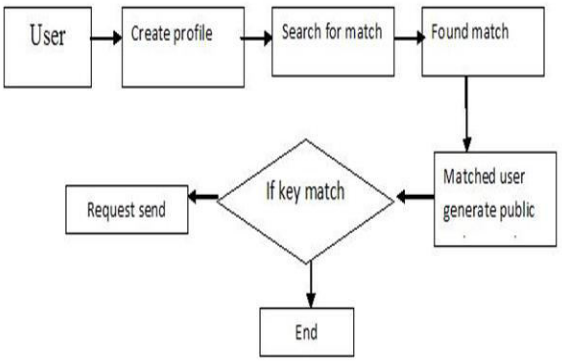
The perpetually increasing dependence on anytime-anywhere availableness of information and therefore the commensurately increasing worry of losing privacy inspire the necessity for privacy-preserving techniques. One inter-esting and customary drawback happens once 2 parties ought to in camera calculate AN intersection of their several sets of information. In doing therefore, one or each parties should get the intersection (if one exists), whereas neither ought to learn something concerning different set components. though previous work has yielded variety of e_ective and stylish

non-public Set Intersection (PSI) techniques, the hunt for e_ciency continues to be current. This paper explores some PSI variations and constructs many secure protocols that area unit ap- preciably a lot of e_cient than the progressive.

III. PROPOSED SYSTEM

In projected System we tend to observe the Mobile web association might not continuously be offered and it should incur high expense. Thus, during this work we tend to specialise in proximity-based localised mobile social networks (MSN) supported short-range wireless technologies like wireless local area network and Bluetooth. The insecure wireless channel and probably untrusted service supplier increase the danger of showing personal data.

IV. SYSTEM ARCHITECTURE



V. MATHEMATICAL MODEL

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 maliciousmessage is blocked user.

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}

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

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 be 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: notification form one OSN to another OSN.

V. CONCLUSION

In this paper, we tend to style a unique radially symmetrical key coding primarily based privacy-preserving profile matching and secure channel institution mechanism in suburbanized MSN with none presetting or trustworthy third party. Many protocols were planned for achieving verifiability and totally different levels of privacy. we tend to analyzed the performance of our protocols and compared them with existing protocols. we tend to conducted in depth evaluations on the performances employing a giant scale dataset from real social networking. The results show that our mechanisms beat out existing strategies considerably and supply economical and secure resolution for mobile social networks. Our economical techniques, together with non-public fuzzy attribute matching and secure channel establishing, may also be applied to several different situations wherever parties don't essentially trust one another, e.g., advertising auction, data sharing and placement primarily based services. In our future work, we'll integrate these techniques into additional networking systems.

VI. REFERENCES

[1] (2013, Oct.). [Online]. Available: http://www.alexa.com/topsites

[2] CNN. (2013, Feb.). Report: Eastern european gang hacked apple, facebook, twitter. [Online]. Available: http://www.cnn.com/2013/02/20/tech/web/hacked-apple-facebook-twitter/index.html

[3] IGN. (2013, Feb.). Microsoft hacked by same method as apple and facebook. [Online]. Available: http://www.ign.com/articles/2013/02/23/microsoft-hacked-by-same-method-as-apple-andfacebook

[4] H. Lin, S. S. M. Chow, D. Xing, Y. Fang, and Z. Cao, "Privacy preserving friend search over online social networks,"

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal

Cryptology ePrint Archive, Report 2011/445. [Online]. Available: http://eprint.iacr.org/2011/445.

[5] R. Zhang, Y. Zhang, J. S. Sun, and G. Yan, "Fine-grained private matching for proximity-based mobile social networking," in Proc.IEEE Int. Conf. Comput. Commun., Orlando, FL, USA, Mar. 2012,pp. 1969–1977.

[6] M. Li, N. Cao, S. Yu, and W. Lou, "FindU: Privacy-preserving personal profile matching in mobile social networks," in Proc. IEEE Int.Conf. Comput. Commun., Shanghai, China,Apr. 2011, pp. 2435–2443.

[7] R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for mhealthcare social network," Mobile Netw. Appl., vol. 16, pp. 683–694, 2011.

[8] X. Liang, M. Barua, R. Lu, X. Lin, and X. Shen, "HealthShare: Achieving secure and privacy-preserving health information sharing through health social networks," Comput. Commun., vol. 35, no. 15, pp. 1910–1920, 2012.

[9] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in Proc. IEEE Int.
Conf. Comput. Commun Shanghai, China, Apr. 2011, pp. 1647–1655.

[10] H. Zhu, S. Du, M. Li, and Z. Gao, "Fairness-aware and privacypreserving friend matching protocol in mobile social networks,"IEEE Trans. Emerging Topics Comput., vol. 1, no. 1, pp. 192–200,Jun. 2005.

[11] E. D. Cristofaro, M. Manulis, and B. Poettering, "Private discovery of common social contacts," in Proc. 9th Int. Conf. Appl. Cryptography Netw. Security, Nerja, Spain, Jun. 2011, pp. 147–165.

[12] M. Nagy, E. D. Cristofaro, A. Dmitrienko, N. Asokan, and A.-R. Sadeghi, "Do I know you?: Efficient and privacy-preserving common friend-finder protocols and applications," in Proc. 29th Annu. Comput. Security Appl. Conf., New Orleans, LA, USA, Dec. 2013,pp. 159–168.

[13] M. J. Freedman, K. Nissim, and B. Pinkas, "Efficient private matching and set intersection," in Proc. 17th Int. Conf. Theory Appl. Cryptographic Techn., Interlaken, Switzerland, May 2004, pp. 1–19.

[14] L. Kissner and D. Song, "Privacy-preserving set operations," in Proc. 25th Annu. Int. Cryptology Conf., CRYPTO'05, Santa Barbara, California, USA, Aug. 2005, pp. 241–245.

[15] C. Hazay and K. Nissim, "Efficient set operations in the presence of malicious adversaries," J. Cryptology, vol. 25, no. 3, pp. 383–433,2012.