ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

An Innovative Group Matching Mechanism Based on Private Set Intersection and Ring Signatures Without Disclosing Any Sensitive Data. (GMATCH(.NET))

Mohd. Abdul Wase Sabahat
M.Tech Student,
Department Of Computer Science Engineering,
KG Reddy College of Engineering & Technology.

Mr. Nagendra Kumar
Assistant Professor,
Department Of Computer Science Engineering,
KG Reddy College of Engineering & Technology.

Abstract:

A social networking site is a platform to build social networks or social relations among people who share interests, activities, backgrounds or real-life connections. A social network service consists of a representation of each user (often a profile), his or her social links, and a variety of additional services. Social network sites are web-based services that allow individuals to create a public profile, to create a list of users with whom to share connections, and view and cross the connections within the system.

Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Social network sites are varied and they incorporate new information and communication tools such as mobile connectivity, photo/video/sharing and blogging. A group (often termed as a community, e-group or club) is a feature in many social network services which allows users to create, post, comment to and read from their own interest- and niche-specific forums, often within the realm of virtual communities.

Groups, which may allow for open or closed access, invitation and/or joining by other users outside the group, are formed to provide mini-networks within the larger, more diverse social network service. In this paper, we studied and implement a new group matching mechanism, by considering private set intersection and ring signatures. With our method, a visitor is able to gather correct group matching information while sensitive information of the visitor and group members are not revealed. In conclusion, we suggest to use batch verification to significantly develop the performance of the matching process.

Keywords:

Privacy, encryption, cloud computing, secure sharing, identity privacy, multi owner, dynamic groups .

Introduction:

Social networking is the practice of expanding the number of one's business and/or social contacts by making connections through individuals. While social networking has gone on almost as long as societies themselves have existed, the unparalleled potential of the Internet to promote such connections is only now being fully recognized and exploited, through Web-based groups established for that purpose. Online community services are sometimes considered as a social network service, though in a broader sense, social network service usually means an individual-centered service whereas online community services are group-centered. Social networking sites allow users to share ideas, pictures, posts, activities, events, interests with people in their network.

The main types of social networking services are those that contain category places (such as former school year or classmates), means to connect with friends (usually with self-description pages), and a recommendation system linked to trust. Popular methods now combine many of these, with American-based services such as Facebook, Google+, YouTube, LinkedIn, Instagram, Pinterest, Vine, Tumblr, and Twitter widely used worldwide; Nexopia in Canada; Badoo, Bebo, Vkontakte (Russia), Delphi, Draugiem.lv (Latvia), Hyves (The Netherlands), iWiW Hungary), Nasza-Klasa (Poland), Soup (Austria), Glocals in Switzerland, Skyrock, The Sphere, StudiVZ (Germany), Tagged, Tuenti (mostly in Spain), Myspace, Xanga and XING in parts of Europe;

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Hi5 and Orkut in South America and Central America; Mxit in Africa; Cyworld, Mixi, Orkut, Renren, Friendster, Sina Weibo and Wretch in Asia and the Pacific Islands. There have been attempts to standardize these services to avoid the need to duplicate entries of friends and interests (see the FOAF standard and the Open Source Initiative). A study reveals that India has recorded world's largest growth in terms of Social Media users in 2013. A 2013 survey found that 73% of U.S adults use social networking sites.

Privacy Issues:

Privacy concerns with social networking services have been raised growing concerns amongst users on the dangers of giving out too much personal information and the threat of sexual predators. Users of these services also need to be aware of data theft or viruses. However, large services, such as MySpace and Netlog, often work with law enforcement to try to prevent such incidents.In addition, there is a perceived privacy threat in relation to placing too much personal information in the hands of large corporations or governmental bodies, allowing a profile to be produced on an individual's behavior on which decisions, detrimental to an individual, may be taken.

Furthermore, there is an issue over the control of data—information that was altered or removed by the user may in fact be retained and passed to third parties. This danger was highlighted when the controversial social networking site Quechup harvested e-mail addresses from users' e-mail accounts for use in a spamming operation.In medical and scientific research, asking subjects for information about their behaviors is normally strictly scrutinized by institutional review boards, for example, to ensure that adolescents and their parents have informed consent. It is not clear whether the same rules apply to researchers who collect data from social networking sites.

These sites often contain a great deal of data that is hard to obtain via traditional means. Even though the data are public, republishing it in a research paper might be considered invasion of privacy.Privacy on social networking sites can be undermined by many factors. For example, users may disclose personal information, sites may not take adequate steps to protect user privacy, and third parties frequently use information posted on social networks for a variety of purposes. "For the Net generation, social networking sites have become the preferred forum for social interactions, from posturing and role playing to simply sounding off. However, because such forums are relatively easy to access, posted content can be reviewed by anyone with an interest in the users' personal information".Following plans by the UK government to monitor traffic on social networks schemes similar to e-mail jamming have been proposed for networks such as Twitter and Facebook. These would involve "friending" and "following" large numbers of random people to thwart attempts at network analysis.

Privacy concerns have been found to differ between users according to gender and personality. Women are less likely to publish information that reveals methods of contacting them. Personality measures openness, extraversion, and conscientiousness were found to positively affect the willingness to disclose data, while neuroticism decreases the willingness to disclose personal information.

Grouping:

Much like electronic mailing lists, they are also owned and maintained by owners, moderators, or managers, which possess the capability of editing posts to discussion threads and regulating member behavior within the group. However, unlike traditional Internet forums and mailing lists, groups in social networking services allow owners and moderators alike to share account credentials between groups without having to log into each and every group. Groups are centered less around discussion forums and common interest, and are more centered around maintenance of a particular geographic location inside the network.

Such groups are often created by the owners of areas such as buildings, plots of land or whole islands in order to cater to the most frequent visitors and patrons of the regions. With the limited asynchronous messaging capability of Second Life, groups are also means of mass-emailing announcements pertinent to the group, but are not completely capable of hosting discussion or deliberation of such announcement messages. Since we've moved a huge part of our social life to the internet online social networking groups has become very important for us to maintain a structure in our social life. Online networking is made up by clusters of people, bounding themselves together on the world wide web.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

To be able to sort out the many different clusters we belong to we use online groups to helps us arrange and make sense of all our contacts. This sense-making is rooted within us, we sort and put people into compartments or sort by categories to make sense and try to understand our relationships to the people around us. Online social networking groups therefore enable us to do the same thing online.

Data in OSNs:

Boyd and Ellison's definition already suggests that OSNs operate on two types of user related data: Profiles: A profile is tied to a user and is their representation to the outside world. Usually this is a self description, or the description of an alter-ego.

Connections :

A connection exists between two users and can be of several types, like friend, colleague, fan, etc. A collection of connections can be represented by a graph.

Behavioral information:

Browsing history and actions undertaken by the user while performing tasks within the OSN. Benevenuto et al. note that this type of meta-data is particularly rich Information such as preferences, friendships or even implicit data such as physical location can be inferred from it. Behavioral data is also found in traditional websites, although behavior there is not related to navigating a social network.

Login credentials:

Most OSNs require, or allow, the user to login to make use of the service. This login information is contained in the login credentials. This is something that can also be found in traditional websites. As said, not all OSNs involve information from all of the categories. This mostly depends on the media-richness of a particular OSN, the functionality it o_ers to users, and its business model. Some information is only available to the OSN (i.e. its software or operators), while other information is also available to (a subset of) the OSN users. Furthermore some information is implicitly supplied to the OSN, by actions taken within the OSN, while other information is explicitly supplied, by providing this information.

Existing System:

Beyond asking for explicit user input, earlier work by Li and Croft focused on handling recency queries, which are queries that are after recent events or breaking news. Li and Croft's time sensitive approach processes a recency query by computing traditional topic similarity scores for each document, and then "boosts" the scores of the most recent documents, to privilege recent articles over older ones. In contrast to traditional models, which assume a uniform prior probability of relevance p(d) for each document d in a collection, Li and Croft define the prior p(d) to be a function of document d's creation date.

The prior probability p(d) decreases exponentially with time, and hence recent documents are ranked higher than older documents. Li and Croft's strategy is designed for queries that are after recent documents, but it does not handle other types of time-sensitive queries, such as [Madrid bombing], [Google IPO], or even [Sarkozy French elections] (in May 2008), that implicitly target one or more past time periods.

Disadvantages:

Previous system difficult to search and joint the group. There is no group verification and batch verification to search.

Proposed System:

We propose a more general framework for efficient way to client can joint the group of social network. We propose a more general framework for handling batch and During the group matching, our scheme should be able to provide the following desirable privacy properties.

Stranger's Attributes Privacy:

The stranger does not reveal any attribute in his profile to any group member.

Group Members' Attributes Privacy:

The stranger only obtains matched attributes that both in his profile and some group member's profile, while the unmatched attributes in group members' profiles are not disclosed to the stranger.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Exact Matching Information Privacy:

The stranger is able to compute group matching information, while any exact matching information between himself and each group member is not revealed.

Advantages:

Security purpose user detail encrypted and decrypted. Implemented the group verification to fast search best group in Social network and user can joint in best group Batch verification increase efficient way to validate the group Group adding also secure way to share the key to add groups,Admin have control to add group and delete group.

Modules:

1.Two-party private matching

2.Multi-party private matching

3.Private matching in social networks

Modules Description:

1.Two-party private matching:

In this paper proposed a private matching scheme, which allows a client and a server compute the set intersection with their own private sets. During private matching, the client only obtains the set intersection while the server does not know any matching result. Agrawal et al. Introduced a private matching scheme between two databases using commutative encryptions. Hazay and Lindell exploited pseudo random functions to evaluate set intersection.

In Dachman-Soledet al. exploited polynomial evaluations to compute the set intersection between two parties, and also leveraged Shamir secret sharing and cut-and-choose protocol to improve efficiency. Recent work in introduced an authorized private set intersection (APSI) based on blind AES signatures. In APSI, each element in the client's set must be authorized by some mutually trusted authority.

2. Multi-party private matching:

In this paper proposed a multi-party private matching scheme to compute the union, intersection and element reduction operations for multiple sets. However, this scheme requires a group decryption among multiple entities, which is impractical between the stranger and group members in social networks.

Ye et al extended previous scheme to a distributed scenario with multiple servers. The dataset of the original server is shared by several sub-servers using Shamir secret sharing. Proposed a private multi-party set intersection scheme based on the two-dimensional verifiable secret sharing scheme.

3. Private matching in social networks:

In this paper focuses on finding the best matched user from the group in mobile social networks. Yang et al. introduced E-Small Talker, which allows users to privately match other people in mobile social networks using the iterative bloom filter (IBF) protocol

CONCLUSION:

In this technical paper, we studied and implemented a new method of matching, Gmatch, a very secure and privacy preserving group matching mechanism in online social networking sites. With the use of this technique, the visitor can effectively gather group matching data/information at the same time as the private information of group members are preserved.

References:

[1] B. Wang, B. Li, and H. Li, Gmatch: Secure and Privatepreserving Group Matching in SocialNetworks, in Proceedings of IEEE Globecom 2012, pp. 744-749, 2012.

[2] M. Li, N. Cao, S. Yu, and W. Lou, FindU: PrivatePreserving Personal Profile Matching in Mobile Social Networks, in Proceedings of IEEE INFOCOM 2011, pp.2435-2443, 2011.

[3] E. Cristofaro and G. Tsudik, Practical Private Set Intersection Protocols with Linear Complexity, in Proceedings of Financial Cryptography 2010, pp. 143-159, 2010.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[4] D. Boneh, C. Gentry, B. Lynn and H. Shacham, Aggregate and Verifiably Encrypted Signatures from Bilinear Maps, in Proceedings of EUROCRYPT 2003, pp. 416-432, 2006.

[5] M. Freedman, K. Nisssim, and B. Pinkas, Efficient Private Matching and Set Intersection, in Proceedings of EUROCRYPT 2004, pp. 1-19, 2004.

[6] P. Paillier, Public Key Cryptosystems Based on Composite Degree Residuosity Classes, in Proceedings of EUROCRYPT 1999, pp. 223-238, 1999.

[7] Z. Yang, B. Zhang, J. Dai, A. Champion, D. Xuan and D. Li, ESmallTalker: A Distributed Mobile System for Social Networking in Physical Proximity, in Proceedings of IEEE ICDCS 2010,pp. 468-477, 2010.

[8] D. Dachman-Soled, T. Malkin, M. Raykova, and M. Yung,"Efficient robust private set intersection," in ACNS '09, 2009,pp. 125–142.

[9] G. S. Narayanan, T. Aishwarya, A. Agrawal, A. Patra, A. Choudhary, and C. P. Rangan, "Multi party distributed private matching, set disjointness and cardinality of set intersection withinformation theoretic security," in CANS '09. Springer - Verlag, Dec. 2009, pp. 21–40.

[10] C. Hazay and Y. Lindell, "Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries," in TCC'08, 2008, pp. 155–175.

[11] S. Jarecki and X. Liu, "Efficient oblivious pseudorandom function with applications to adaptive ot and secure computation of set intersection," in TCC '09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 577–594.

[12] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in IEEE INFOCOM '11, Apr 2011, pp. 1–9.

[13] E. De Cristofaro, M. Manulis, and B. Poettering, "Private discovery of common social contacts," in Applied Cryptography and Network Security. Springer, 2011, pp. 147–165.

[14] E. De Cristofaro, A. Durussel, and I. Aad, "Reclaiming privacy for smartphone applications," in Pervasive Computing and Communications (PerCom), 2011 IEEE International Conference on,march 2011, pp. 84 –92.

[15] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation."

[16] R. Gennaro, M. O. Rabin, and T. Rabin, "Simplified vss and fast-track multiparty computations with applications to threshold cryptography," in ACM PODC '98, 1998, pp. 101–111.

[17] T. Nishide and K. Ohta, "Multiparty computation for interval, equality, and comparison without bitdecomposition protocol," in PKC'07, 2007, pp. 343–360.