International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Survey on Privacy Preserving in Social Networks

S. Mayil[1], Dr. M. Vanitha[2]

[1]Research scholar, PG & Research Department of Computer Science,
JJ College of Arts and Science (Autonomous), Pudukkottai, Tamil Nadu, India

[2]Assistant Professor, Ph.D. and Research Department of Computer Application, Alagappa University, Karaikudi , Tamilnadu.

Abstract: ***The development of online social networks and the release of data network resulting in the risk of leakage of personal confidential information. This requires privacy protection before the data network is published by the service provider. Data privacy online social networks are important in recent years. Therefore, this research is still in its infancy. This article describes the generalization techniques of anonymous social networking data with sufficient privacy for harsh environments while preserving the validity of the data. The loss metric information, iloss, is used to check the information due to the loss of the generalized amount. While these networks make frequent data sharing and intercommunication between users can instantly and privacy problems that may arise are very explicable with their obvious immediate consequences. Although the concept of privacy can take different forms, the ultimate challenge is how to prevent the invasion of privacy when personal information is available. Basic social networks, co-statements, and their associated primary motivations. The following describes how to protect privacy, relying on technical analysis and link social networks to disclose sensitive user information.***

Keywords: Data Privacy, Data Publishing, Privacy Preserving, Social Network, Service Provider.

1. Introduction

Online social networks are becoming increasingly popular for people to sign up for social media or social networking sites. This generates a large amount of user data collected and maintained by the social network service provider. Data generated through social networking services is known as social networking data being published for others in certain circumstances. One is when the need arises and the other is that the owner of the data must be shared with a third party, such as an ad partner's data useful for a specific analysis of the data, which is generally accepted as part of the policy subscriber. These data contain other valuable information about the user who helps in positioning a better social ad. Social network analysis is the modernization of sociology, geography, economics and information science are being used. Researchers in various fields use these data for different purposes, and government agencies need researchers from social network information and safety data. Therefore, the required data are shared or published in all of the above cases. Data owners can publish to others for analysis, but can create a serious threat to privacy. We propose a privacy-safe data exchange scheme for maintaining online social networks. The main objective of the proposal is to ensure data privacy and access control to private data stored in the storage of potential United Nations trusts. In addition to ensuring data privacy and access control, our program is designed to allow safe and efficient searches through data sharing, and to support frequent replacement of members dynamically enough to revoke a social group.

In order to meet the needs of online data, online social media operators have been sharing collections and third party applications with third-party applications and data maintained with third-party applications such as ad, application developers, and academic parties such as Facebook The exponential growth of this number. Social network data contains sensitive and confidential information about users. Thus, in its original form, the exchange of these data may affect the privacy of individuals. Personal privacy is defined as "an individual's decision as to what information about himself should be communicated to others and in what context is correct." When providing an adversary the user privacy and confidential information about privacy violations occur. In order to maintain the privacy of individuals, the data collected from users of the publication is an important area of research.

2. Related Work

Cryptagram designs, implements and evaluates systems designed to enhance the privacy of online photos. Cryptagram allows users to convert photos to OSN encrypted images uploaded by users. The administrative user accesses these photos independently of the OSN or other third party's direct control via a shared secret. The OSN application converts standard images (JPEG compression) to all loaded images, so Cryptagram provides encoding and image encryption mechanisms that are tolerant of these changes. Cryptagram ensures that the correct credentials can be used by the recipient to fully recover the transform, while the NBS can not deduce that the original image is loaded with the version of the encrypted image of the original image. The browser extension Cryptagram integrates seamlessly with existing National Statistics offices, including Facebook and Google+, and currently has more than 400 active [1] users. There are many types of information shared by users as images, messages, audio, video, etc. The amount of online social network that provides security when uploading pictures is less. Thus, an information filtering method can be used to filter information in an online social network. In social networks, information filtering is very expensive and difficult to process due to the various functions included in these social networks. We can provide a method of protecting the privacy of the predicted image privacy policy according to the adaptability of the chosen user according to the method of different social background users. The purpose of this work is to design the framework, called the Filter Wall

Licensed Under Creative Commons Attribution CC BY

(FW), to filter out unwanted wall user OSN messages. The most important effort is to achieve short text categorization (STC) used to extract and select marker annotations. Then, using the filter and block list rules, remove unwanted messages and prevent any unwanted messages from being sent continuously by the server to automatically filter the friends [2].

The user profile matches the privacy of the mobile social network saved (MSN), and provides a new set of profiles for matching profiles. First, we intend to compare the overheads based on comparative cost (eCPM) protocols, which run between the initiator and the responder. It proposes an implicit comparison protocol based on Contour Contrast (ICPM), which allows the initiator to obtain some information instead of directly comparing the results of the response. Messages in unrelated user profiles can be classified into several types by the reply. The initiator implicitly selects that the open group is an unknown response. The response is prepared in two columns per class, and the initiator can only get a message based on results similar to those in a single attribute. The generalized ICPM-to-predicate-based contour matching (IPPM) is then included, which allows multiple similarity criteria to contain multiple attributes. The analysis shows that all of these secrets achieve the privacy profile of the user profile. In addition, eCPM revealed similar results for the initiator and provided only a relative anonymity; IPTPM and IPPM could not disclose all the results and provide a completely anonymous (secret). The communication overhead and robustness of the anonymous protocol are analyzed. Then submit an improved version of eCPM, called eCPM +, based on the predictive pseudonyms of a new adaptive shift strategy combined with eCPM. ECPM performance and eCPM + are based on a wide range of tracking-based simulations. The simulation results show that per1000 impressions + achieves a significantly greater number of anonymity and pseudonyms per thousand impressions [3].

NOYB provides privacy and retains the online dictionary function using the secret dictionary. The privacy profile data may be fixed to the NOYB, and the user's privacy (i.e., user relationships and interactions) is not protected [4]. [5] proposed the use of graphics on Facebook to establish a photo-based authentication framework. [4] Utilize homomorphic encryption to allow indirect access to social relations resources, without the trust of third parties, to protect private users of social relations facilities owners. Recently, OSN preserves peer-to-peer (P2P) privacy [6], [7]. Other studies [8] - [11] focus on different security issues, such as Siebel attacks and anonymity in general social networks. Privacy and anonymity, extensively studied many other data sharing networks, such as the crowd [12], and significant P2P networks such as Freenet [13] and Taishan [14].

Use minor minutiae anonymous schemes that match the minimum DFS code. The scheme sub charts matches the labels used to find related sub graphs in the graph and anonymize the sub graphs. The downside of this scheme is that it cannot actually be implemented in social networks with real life on thousands of nodes and sides. Only consider neighbors. By increasing the number of nodes by more than one size exponentially growing neighbors [15]. Recent work has increased near the size of the upper three [16]. However, these methods [15], [16] and therefore cannot be applied to the size of social networks, making them almost impossible.

3. Privacy in Social Networks

The author considers an attack on an anonymous network. In their model, there are only network consists nodes and edges. Detail values are not included. The purpose of the attacker is very simple, is to identify people. Also, the problem is that in considering this work, because they ignore the details and do not take into account the impact of personal data privacy is very different.

However, it is our job to deduce data from nodes in the network, not separately, to protect privacy individuals. They identify data network interference. Although his approach takes into account the graphical structure, does not account for any additional details, or a node in the social network may have the function.

Data network perturbation protection privacy although his approach takes into account the graphical structure, one does not think that a node in a social network can possess. The authors propose several methods of anonymous social graphs, focusing on the details of the idea being anonymized and the features in that group, and thus an anonymous graphic as a whole. However, their approach focuses on the anonymous structure itself. For example, by using the K-anonymous or un-area depending on the quasi the sounder is selected to authenticate, and most of the data may be lost in uniqueness. By keeping us anonymous, we maintain the uniqueness of each node in the completion, allowing for more information after the report is published.

4. Privacy Preservation via Generalization

In order to protect privacy, anonymity and other randomization methods are modified by adding / removing edges to the graphic structure, and then releasing the detailed chart. Unlike the first two methods, the method can be considered to be a so-called super-node of the large sand edge in the partitioned nodes and the edge is basically like a generalized grouping. The idea of generalization has been adopted in the anonymous form of data has been well adopted. For the data on the social network, the properties of the original graphic macros can still be studied using the links between the partitions that describe the complete partition, and the generalized graph structure.

5. Challenges in Preserving Privacy in Social Network Data Publishing

Ensuring privacy for social network data is difficult than the data

a) Modeling background knowledge is a formidable opponent of data from social network microforms. In micro format data, the user links the quasi-identifiers in the social network information from various sources such as vertices and edges, and the sub graph and the nearby

Licensed Under Creative Commons Attribution CC BY

graphic labels can be used to identify the personal recognition.

b) The loss of information is an indicator of the amount of distortion measured. The sum of information loss of each record that can be used for microform data loss. Because the social network is a graphical structure with a set of vertices and edges, it is difficult to compare the vertex and edge social networks by comparing them individually. Anonymous social networks and primitive social networks have the same number of vertices and edges can have very different properties such as mediation, connectivity and diameter. The information and anonymous quality loss can be measured in different ways.

c) Technological development maintaining the confidentiality of social network data is difficult relational data. Flake micro data uses anonymous anonymity techniques, while social network nodes and edge structures, any change in the label or edge can have the effect of proximity to other vertices and edges.

Existing models maintain the privacy of micro data that has been used for social networking data. This work has been done using K-anonymous, L-diversity and integrated K-L-anonymous diversity to protect user data in ways that have been published online by some researchers. The social network data is represented as where each node / vertex represents a separate graph. The unstructured data and the edges represent the links / associations between the nodes.

Preservation Technology Privacy has been developed taking into account the following:
1. Opponent's understanding
2. The validity of the data after publication

Thus, according to the knowledge of the enemy target node used to attack the following technologies have been developed using K-anonymity to differentiate the researchers from the public view of the disclosure of the data published in the social network. It has been assumed that opponents possess the knowledge of the degree of personal destiny and the proximity of the target. It presents a practical solution to attack against the background knowledge. The anonymous social network obtained by this method can be used for web queries that are used with great precision.

6. Conclusion

Privacy and security are important issues in many areas of the computer. Especially in the areas of social networks are particularly interested in online, due to the sensitive data involved. Never before had a collection of personal identities been sensitive to data like we are now available with online social networks. The integration of these data is very dangerous. For example, home and birth dates are deemed necessary to determine your social security number for more reasonable accuracy, which is often easy to get online on a user profile on a social network.

This paper presents a study of various techniques and algorithms proposed by previous researchers to provide better access to online social network data privacy protection. From the above studies, some of the social networks that access data online at the same time are available. Or lack of management support Multi-party privacy mainstream social media The existing infrastructure means that users can not fully control to these elements are actually not shared. Computing mechanisms that can combine multiple users' privacy preferences into a single policy can solve the problem. However, consolidating the privacy preferences of multiple users is not an easy task, because privacy preferences may conflict and therefore conflict resolution is required. In addition, these methods should take into account how the user may be in conflict resolution in order to propose a solution that is acceptable to all users of the project to be truly shared.

References

[1] Matt Tierney, Ian Spiro, Christoph Bregler, Lakshminarayanan Subramanian by "Cryptagram: Photo Privacy for Online Social Media", 2013.
[2] M. Muthubrindha, Dr. A. Valarmathi by "Privacy Based Image and Comment Sharing on Online Social Networks Based on Short Text Classification", IJARCSE Volume 6, Issue 4, April 2016.
[3] Kundan Shewale, Sachin D. Babar by "An Efficient Profile Matching Protocol Using Privacy Preserving In Mobile Social Network ",7th International Conference on Communication, Computing and virtualization 2016
[4] S. Guha, K. Tang, and P. Francis, "NOYB: privacy in online social networks," An ACM SIGCOMM 2008 Workshop (WOSN'08), pp. 49–54,2008.
[5] S. Yardi, N. Feamster, and A. Bruckman, "Photo-based authentication using social networks," An ACM SIGCOMM 2008 Workshop (WOSN'08), pp. 55–59, Aug. 2008.
[6] L. A. Cutillo and R. Molva, "Safebook: a privacy-preserving online socialnetwork leveraging on real-life trust," IEEE Communications Magazine,vol. 47, no. 12, pp. 94–101, Dec. 2009.
[7] S. Buchegger, D. Schi¨ oberg, L.-H. Vu, and A. Datta, "PeerSoN: p2p social networking," Proc. 2nd ACM EuroSys Workshop on Social Network Systems, pp. 46–52, 2009.
[8] G. Danezis and P. Mittal, "Sybilinfer: detecting sybil nodes using social networks," in Proc. Network and Distributed System Security Symposium (NDSS), Feb. 2009.
[9] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "Sybillimit: a near-optimal social network defense against sybil attacks," in Proc. IEEE Symposium onSecurity and Privacy, pp. 3–17, Oct. 2008.
[10] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard: defending against sybil attacks via social networks," SIGCOMM, Computing Communication Review, vol. 36, no. 4, pp. 267–278, 2006.
[11] C. Diaz, C. Troncoso, and A. Serjantov, On the impact of social network profiling on anonymity, in N. Borisov and I. Goldberg (Eds.): PETS 2008,LNCS 5134, 2008.
[12] M. Reiter and A. Rubin, "Crowds: anonymity for web transactions," ACM Transactions on Information and System Security, vol. 1, no. 1, pp. 66–92, June 1998.
[13] "The freenet project," http://freenetproject.org/.
[14] M. Freedman and R. Morris, "Tarzan: a peer-to-peer anonymizing network layer," in ACM Conference on

Licensed Under Creative Commons Attribution CC BY

Computer and Communications Security (CCS), pp. 193–206, Nov. 2002.
[15] Liu, L., Wang, J., Liu, J. and Zhang, J."'Privacy preserving in social networks against sensitive edge disclosure", Technical Report CMIDA-HiPSCCS 006-08, Department of Computer Science, University of Kentucky, KY, 2008.
[16] Tripathy, B.K. and Panda, G.K. "A new approach to manage security against neighborhood attacks in social networks", International Conference on Advances in Social Networks Analysis and Mining (ASONAM), pp.264–269 9–11 August, Odense, 2010.
[17] J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy for social networks," in Proc. Symp. Usable Privacy Security, 2009.
[18] A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P. Tsang, "Social circles: Tackling privacy in social networks," in Proc. Symp. Usable Privacy Security, 2008.
[19] P. Klemperer, Y. Liang, M. Mazurek, M. Sleeper, B. Ur, L. Bauer, L. F. Cranor, N. Gupta, and M. Reiter, "Tag, you can see it!: Using tags for access control in photo sharing," in Proc. ACM Annu. Conf. Human Factors Comput. Syst., 2012, pp. 377–386.
[20] A. Mazzia, K. LeFevre, and A. E.,, "The PViz comprehension tool for social network privacy settings," in Proc. Symp. Usable Privacy Security, 2012.

Licensed Under Creative Commons Attribution CC BY