Graph Terminologies to Enhance the Security of SNS

Ashish Shah[1], Dr. Abha Khandelwal[2]
Department of Computer Science
[1, 2]Hislop College, Nagpur

Abstract-*With the wide spread of Online Social Site and the popularity of such site among all type of users. The privacy concern related to such Online social site has increased. The bulk amount of data uploaded on such site has brought an issue related to data security. We in this papers focus on such popular social sites and the security risk on such site. In this paper we try to study the general issue faced in using such sites and try to combine the graph terminology in social site. We try to explain the architecture of such site using graph. Thus to enhance the security in such online site we use some graph terminology.*

Keywords*-*Social Networking Site, Privacy, Data Security, Graph, architecture.

I. INTRODUCTION

Online Social networking has become a new way of being connected. One of the biggest milestone of web 2.0. Since the introduction of Social networking site it has gained its popularity amongst all category of users. Social networking sites have changed the way we communicate and interact with other users. Such sites have given a platform to users of same area of interest or liking to communicate and share online. With the grate popularity as top social site has millions users have attracted many service provider to develop site with verity of features to connect. SNS has a huge amount of users data, some of it he may want to use share and some want to keep hidden this come a area of concern[1]. All general social site provide setting for user to keep their data secured but it is found users still face issue on such site. We try to study the privacy strategy used by the social networking sites. We co-relate Graph theory and SNS to enhance the current security model of such sites, which are not up to the mark[2].

II. PROBLEM DEFINATION

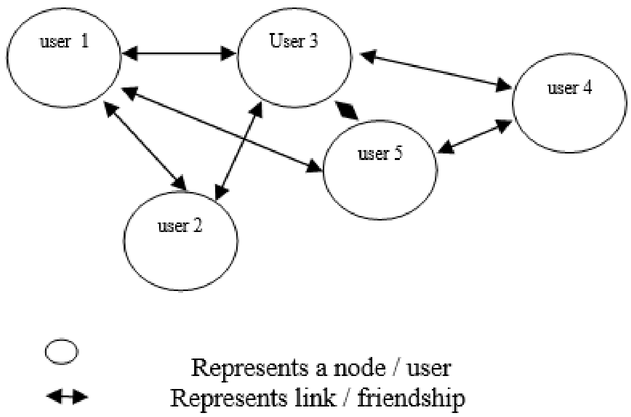
Since SNS are widely in demand of current scenarios, the threat of their usage has also greater than before. Due to the negligence of user and presence of less privacy protection tools, huge amount of user’s data, including user’s personal information, pictures and videos, is at risk. They can be used by strangers, recruiters and even the public at large, in any way in which they want. Despite of such major research work going on in this area security services have failed to solve all the privacy risks. Our research work is to provide some additional Privacy Policies that are used to enhance the existing Privacy Policies of Social Networking Sites. We try to merge the technical terminology of graph to improve the security of online social sites.

III. LITERATURE SURVEY

We try to study some of the proposed security models and the loop holes in them, Singh et al. propose the xBook framework for building privacy preserving so¬cial network applications [3]. xBook uses information flow models to control what un trusted applications can do with the information they receive. xBook provides enforcement for both user-user access control for informa¬tion flow within a single application, as well as for information sharing with entities outside xBook. Social network site are re-designed to have access to all the data that they need, but this data is not allowed to be passed on to an external entity unless approved by the user. However, xBook does not perform encryption for data confidentiality and hence the security and privacy risks persist. Cristofaro et al. propose Hummingbird, a privacy enhanced version of Twitter type social network [4]. In this architecture, users encrypt their tweets and can follow hash-tags without revealing this information to unau¬thorized parties. Hummingbird is a centralized online social networking design and the service provider does not have access to the tweet contents because of encryption, which may not motivate it to store user data. Lucas and Borisov propose flyByNight, a Facebook application designed to mitigate privacy risks in social networks [5]. flyByNight users encrypt sensitive messages using javascript on the client side and send the ciphertext to some intended party, i.e., Facebook friends, who can then decrypt the data. The architecture ensures that transferred sensitive data cannot be viewed by the Facebook servers in an unencrypted form. However, the utility of flyByNight is limited to preserving the privacy of messages intended for social network friends, i.e., email type communication, and thus, it does not provide complete privacy. For example, the application server knows a user's friendlist on facebook. flyByNight is also vulnerable to active attacks by the OSN provider, since the OSN interface is used for key management. Guha et al. propose to improve user privacy while still preserving the func¬tionality of existing online social network providers [6]. Their structural design is called none of your business (NOYB), in which encryption is used to hide the data from the untrusted social network provider. The key feature of their architecture is a general cipher and encoding scheme that preserves the se¬mantic properties of data such that it can be processed by the social network provider oblivious to encryption. Frikken describes a key allocation scheme for OSNs [7]. In this work, relationship between two users depends on their distance. Luo et al. propose FaceCloak where users store random and fake data on Facebook and the actual data in encrypted form on FaceCloak server [8]. Fake data from Facebook is used as an index to retrieve actual data from FaceCloak on the client side. This design introduces redundant data storage at two different servers. Beato et al. propose Scramble, which uses symmetric key encryption to provide data confidentiality and integrity [9]. However, Scramble model do creates an access control list of users who are actually allowed to see a piece of data by encrypting the symmetric key to each of them separately. Hence, the approach is not expressive. The fact to make a balance between, the freedom to give user to share and communicate and on other hand to keep user data secure is difficult.

IV. GRAPHICAL REPRESENTATION OF SNS

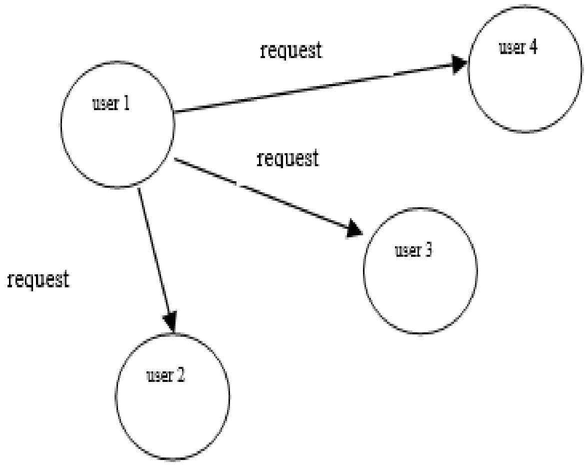
As we know Graph is a pictorial representation of a set of objects where some pairs of objects are connected by links. The interconnected objects are represented by points termed as vertices, and the links that connect the vertices are called edges. Thus structure like Online social sites can be perfectly represented in graph like structure. For such representation we can assume each user as a node of a graph. As nodes are connected to one another with link call vertices we can correlate it with user to user connection call friends in terms of facebook. Each user if assumed as node can be connected to one or more the one users who is further connected to other users in social sites. Diagrammatic representation can be shown as below.



As shown in figure structure of a online social site such as facebook can be represented as a by directional graph.

V.PROPOSED POLICIES AND IMPLEMENTATION

As discussed structure of online social sites can be representation as graph. Thus all the terminologies of graph too perfectly fit the representation of structure of online social sites. Online networking has loops, parallel nodes or users[10]. We can also correlate an isolated node with social sites, users not connected to any one. Thus to enhance the security of online social site we focus the concept of in degree and out degree of graph[11]. We suggest that is a node has all out degree by sending request and zero or less in degree the node or user can be considered as fake or un trusted user.



As we can see in fig a user 1 try to send request to n number of user its out degree if taken as request is greater. Where as its in degree is zero as no one knows this user1 thus no request is towards such users. Such users can be a consider as area of censor. Such methodology can be added to enhance existing security of online social networking.

VI. CONCLUSIONS

Social networking site have become an addiction amongst youth. It has become a part of their status. Thus the data which shared by user can't be controlled. Users knowingly un knowingly share upload data. Thus a social site have work on their security models equally as they provide new features in there site. Such model that makes a balance between being connected and secured. Graph representation can be considered as effective and efficient way to add security features to current security of online social sites.

REFERENCES

[1] Lujun Fang and Kristen LeFevre, "Privacy Wizards for Social Networking Sites" April 26-30 NC.U.S.A. p. 351-360.

[2] SONIA JAHID," SOCIAL NETWORKING: SECURITY, PRIVACY, AND APPLICATIONS" 2013.

[3] K. Singh, S. Bhola, and W. Lee, "xBook: Redesigning Privacy Control in Social Networking Platforms," in USENIX Security, 2009.

[4] E. D. Cristofaro, C. Soriente, G. Tsudik, and A. Williams, "Humming¬bird: Privacy at the Time of Twitter," in IEEE S & P, 2012.

[5] M. M. Lucas and N. Borisov, "FlyByNight: Mitigating the Privacy Risks of Social Networking," in WPES, 2008.

[6] S. Guha, K. Tang, and P. Francis, "NOYB: Privacy in Online Social Networks," in WOSN, 2008.

[7] K. B. Frikken, "Key Allocation Schemes for Private Social Networks ," Social Networks, pp. 11-19, 2009.

[8] W. Luo, Q. Xie, and U. Hengartner, "FaceCloak: An Architecture for User Privacy on Social Networking Sites," in PASSAT, Aug. 2009, pp. 26-33.

[9] Beato, Filipe and Kohlweiss, Markulf and Wouters, Karel, "Scramble! Your Social Network Data." in PETS, 2011.

[10] seymour lipschutz, "data Structures" .

[11] debasis samanta , "classic data structures".