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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Privacy Management of Data Publication on Social Networks

Shahana Beegum K [1], Reshmi T.S [2]

P.G. Student, Department of Computer Engineering, Cochin College of Engineering, Valanchery, Kerala, India[1]

Associate Professor, Department of Computer Engineering, Cochin College of Engineering, Valanchery, Kerala, India[2]

ABSTRACT: Nowadays the world is connected to the Internet and the social networks have important role in our everyday life, so security and privacy is must. The online social networks have clear picture that shows the users social relationships. The user shares their current status and updates their information about personal lives. The privacy risks for such activities are more, such as disclosure of their personal information to public than planned. Also, they post information about others without their permission. The lack of experience and unconscious about social networks services continue the situation. So, propose an automated system that would protect the user's identity and also helps to share the posts and images without losing users privacy to the public. And the proposed method allows send messages and photos privately as messages to their friends while posting their timeline, which provide more privacy than the existing approaches.

KEYWORDS: Online Social Networks (OSNs), Latent Dirichlet Allocation(LDA), privacy preserving, social media.

I. INRODUCTION

Recently we can see the exponential growth in social media. Such as Facebook, can used to illustrate the social relationships where it has hundreds of millions of active users and shared items including stories, new posts, personal information, photos etc. The Online Social Networks provides each user with their own space containing their profile information, friend list, list of photos, web pages such as in Facebook timeline where friends and users can post the messages.

A user's profile includes all information usually contains user's interest, work information, birthday, qualification, place, email address. In existing approaches users cannot hide the personal information from unwanted individuals, only they can hide their timeline. Hence we proposed an automated system that can help us to provide more security than existing approach. In this proposed system when a user searches for a friend, they can only their account with profile picture with request and chat option. The other details will be hidden using concept of Latent Dirichlet Allocation (LDA) algorithm. Also, the system helps us to send messages and photos personally by using a public message option. When a user want to post a message or a photo in timeline, maybe it will be passed to others timeline by liking, commenting or tagging.

Sometimes, we do not like to pass some posts but also we like to share the information to our friends. So we use an option for public message which leads to send our message or photos to all friends in our friends list. Currently by posting messages or images may liked by friends, which will showed in their friends wall that they would liked who are not friends of us. Thus, may they will check our profile. So it will lead to disclosure our privacy. Here, we implement an automated way to secure our privacy without manual intervention.

II. RELATED WORK

There are different methods proposed for photos and message sharing[4][7]. Also, identity disclosure is familiar problem in social networking applications. The recent related proposed systems are to resolve multi-party privacy conflicts in social media. The existing approaches are considering only fixed number of ways to aggregating users privacy preferences without considering the users willingness to sharing the messages and photos by applying only

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

their sharing preferences of the user (e.g., Veto voting). The users are forced to done manually, which increase the burden on the user. Also the manual negotiation consumes the time. In voting method the user need to check every users involved in a photo or message when tagged. The main issue faced by the user, done manually which consumes the time. The third party is needed to collect each decision involved in an shared item. In[11] the users manually define the privacy settings for each item they would upload. Also they need to define the sensitivity for the item and their priority to friends. The privacy risk is to calculate these parameters, then they define the conflicting target users on sharing. In [6] the authors proposed a user interaction model, which lets the users to control over the default privacy settings. They present the knowledgeable way for setting default privacy policies for unexperienced and unconscious users. In [5] the authors proposed a mechanism for rethinking the access control. The proposed method allows to prevent unwanted individuals from recognizing users in photos. When another user try to access the photo, the system determines which faces do not have permission to access. Also, the blurred photos of users cannot shared while others are try to share. Thus, it cannot share a photo when there is a blurred face and face is used as user identification.

The remainder of the paper is organized as follows. Section 3 presents the proposed method. The experimental results in Section 4. Finally, conclusions are given in Section 5.

III. PROPOSED METHOD

The proposed system provides more privacy for users in social networks in an automated way using LDA. In this paper, proposed a method for protecting personal information about user and sharing of messages and photos with friends without losing privacy.

Framework consists of two processes:

- Web application development
- Implementation of LDA algorithm to hide users profile and sending option while posting images and messages on timeline.

The first step involves creation of web application in client side. The home page contains the login section which includes user name and password for already registered users and registering option for starting users, for entering to the application.

During the development phase, the user data recorded to database. The user activities are accessed from database. The LDA algorithm concept is used in implementation. For hiding the users profile information for unwanted individuals, the user do not need to setting the privacy section manually. The system will done automatically. Also, the system will send the messages and photos to all friends of users without selecting and making groups of friends while posting to the timeline.

Each registered user can login to the system and send request to make friends. Only after having the friendship the user can allow view their profile and other information. Then the user can send messages or share items to friends by selecting them as seen in existing systems. Also, the can share their items using public option, which sends items to each of friends in the friend list. The proposed system helps to make keep in contact with every time.

The others can make request and send messages which are seen as conflict chats to the users. When they are trying to search the user, only chat and send request option will be produced. The users profile and other information will not available for others, which ensures the security.

In proposed method, implementing phases follows the areas in data mining for an efficient system:

- Integrating and mining biodata- Integrate and mine biodata from multiple users to decipher and utilize the structure of biological networks to shed new insight on the functions of biological system. We have expanded and integrated the techniques and methods in information acquisition, transmission and processing for information in networks. We have developed the methods for semantic-based data integration, automated hypothesis generation from mined data and automated scalable analytical tools to evaluate simulation results and refine models.
- Big data fast response- Proposed to build a stream-based big data analytic framework for fast response and real-time decision making. Designing big data sampling mechanisms to reduce to big data volumes to a manageable size for processing. Building prediction models from big data streams which can adaptively adjust to the dynamic changing of the data, as well as accurately predict the trend of data in the future.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

- Pattern matching and mining- Performs a systematic investigation on pattern matching , pattern mining with wildcards and application problems
- Key technologies for integration and mining- Performs an investigation on the availability and statistical regularities of multisource, massive and dynamic information including cross media search based on the information extraction, sampling uncertain information querying and cross-domain and cross-platform information polymerization. To break through the limitations of traditional data mining method.
- Group influence and interactions- Employing group influence and information diffusion models and deliberating group interaction rules in social networks using dynamic game theory which helps to studying interactive individual selection and effect evaluation under social networks affected by group emotion, analysing emotional interactions, influence among individuals and groups, establishing an interactive influence model and its computing methods for social network groups, to reveal the interactive influence effects and evolution of social networks.

IV. EXPERIMENTAL RESULTS

This section shows the experimental results of the proposed method. First user login to the accounts, and searching for friends. If the searched person is already friend can communicate, if not then provide only a chat option while providing the timeline of the searched person.

The user can search friends for making friends in social networks by sending requests. Also, by searching for a friends provides only chat option while providing their timeline and details. Figure 1 shows the examples of searched person account.

Figure 1. Searching friends

The user communicates with friends by messages. For a searched person the user can send messages and it will put on conflict chat. Figure 2 shows the examples of searched person account, is stored as conflict chat in database.

Figure 2. Conflict chat

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

The user details and shared items are stored in database. Figure 3 shows the sharing of messages and photos with friends publicly and privately. By sharing using public message the system help to send messages every friends of the user without selecting. Thus the user shared items will protected from public.

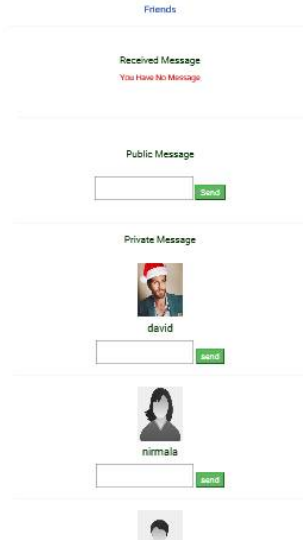

Figure 3. Sharing page

The consuming time and security of the proposed privacy preserving technique performance is demonstrated using figure 4. In this diagram the X axis shows the methods on which the experimentation is performed, and Y axis contains the time in terms of seconds.

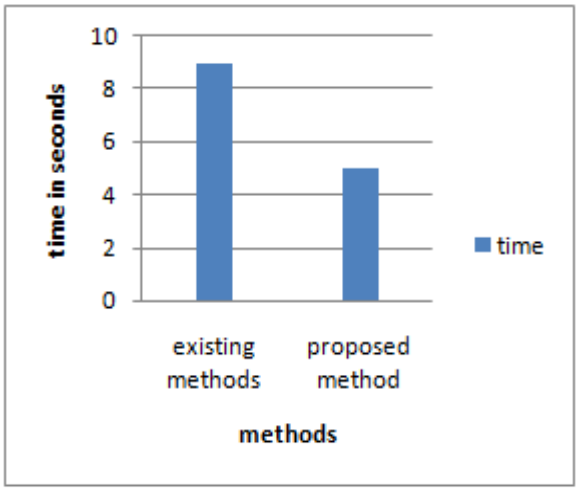

Figure 4. Time taken graph for existing and proposed methods

Security demonstrated using the figure 5. In this diagram the X axis shows the methods and Y axis contains the privacy in terms of percentage. Our system provides more security than existing approaches.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

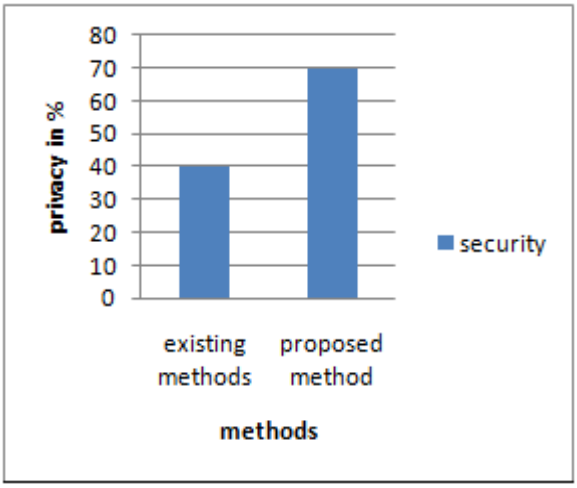

Figure 5. Security in terms of privacy for existing and proposed methods

V. CONCLUSION

In this approach we implement a secured way to sharing messages and photos with friends and preserving of user details from public. The privacy preserving of the users details is important in social networks. In proposed method we implement a method for share message post and photos securely with friends without disclosing to the public which is different from existing approaches. Also, implement the method to hide personal information of users for public without manually settings, and this method used as a friend book, which can share the messages to every friends in list without selecting while posting on timeline. In future may extend with sharing of audios and videos.

REFERENCES

1. Jose M. Such and Natalia Criado, "Resolving Multi-Party Privacy Conflicts in Social Media", IEEE transactions on knowledge and data engineering, vol. 28, pp. 1041-4347, July 2016.
2. Hongxin Hu, Gail-Joon Ahn and Jan Jorgensen, "Multiparty Access Control for Online Social Networks: Model and Mechanisms", IEEE transactions on knowledge and data engineering, vol. 25, pp. 1614-1627, July 2013.
3. Squicciarini, M. Shehab, and F. Paci, "Collective privacy management in social networks", in WWW, pp. 521-530, April 2009.
4. K. Thomas, C. Grier, and D. M. Nicol,, "unfriendly: Multi-party privacy risks in social networks", in Privacy Enhancing Technologies, pp. 236–252, 2010.
5. P. Ilia, I. Polakis, E. Athanasopoulos, F. Maggi, and S. Ioannidis, "Face/off: Preventing privacy leakage from photos in social networks", in Proceedings of the 22nd Conference on Computer and Communications Security(CCS), pp. 781–792, 2015.
6 .E. Toch, N. M. Sadeh, and J. Hong, "Generating default privacy policies for online social networks", in CHI'10 Extended Abstracts on Human Factors in Computing Systems, pp. 4243– 4248, 2010.
7. A. Besmer and H. Richter Lipford, "Moving beyond un tagging: photo privacy in a tagged world," in ACM, pp. 1563– 1572, 2010.
8. J. M. Such and M. Rovatsos, " Privacy policy negotiation in social media", ACM Transactions on Autonomous and Adaptive Systems, 2015.
9. H. R. Lipford, A. Besmer, and J. Watson, "Understanding privacy settings in facebook with an audience view", in UPSEC proc. of the first conference on usability, psychology, and security, pp. 1–8, 2008.
10. J. M. Such, A. Espinosa, A. Garcia-Fornes, and C. Sierra, "Self disclosure decision making based on intimacy and privacy", In Information Sciences, vol. 211, pp. 93–111, 2012.
11. H. Hu, G.-J. Ahn, and J. Jorgensen, "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks", in Proc. ACSAC'11 proceedings of the 27th Annual Computer Security Applications Conference, pp. 103–112, 2011.
12. J. M. Such and M. Rovatsos, "Privacy policy negotiation in social media", ACM Transactions on Autonomous and Adaptive Systems, vol. 11, 2015.