International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 2 521 - 523

A Survey on Securing User Data in Social Networks using Privacy Preserving Options

Priyanka Thakare
Department of Computer Science and Engineering
G.H. Raisoni Institute of Engineering and Technology for Women, Nagpur, India
thakarepriya89@gmail.com

Hemlata Dakhore
Assistant Professor, Department of Computer Science and Engineering
G.H Raisoni Institute of Engineering and Technology for Women, Nagpur, India

***Abstract*—** Privacy is one of greatest rubbing focuses that rises when interchanges get interceded in Online Social Networks (OSNs).different groups of software engineering analysts have been surrounded the 'OSN security issue' as one of the observation, institutional or social protection. On account of handling these issues they have likewise treated them as though they were free. The principle contends is that the diverse security issues are snared and that the examination on protection in OSNs would profit from a more all encompassing methodology. In this paper, we first give a prologue to the observation and social security viewpoint stressing the account that the educate them, and their suspicions, objectives and techniques.

*****

I. INTRODUCTION

On-line interpersonal organization applications seriously experience the ill effects of different security and protection exposures. Protection is one of the grating focuses that rise when interchanges get intervened in Online Social Networks (OSNs). Distinctive groups of software engineering scientists have surrounded the 'OSN security issue' as one of observation, institutional or social protection. In handling these issues they have likewise treated them as though they were free. These requirements for a better grain and more customized security in information distribution of informal organizations. Because of the prevalence of informal organizations, numerous recommendations have been proposed to ensure the security of the systems. All these works accept that the assaults utilize the same foundation information. On the other hand, in practice, distinctive clients have diverse security secure prerequisites. Accordingly, accepting the assaults with the same foundation information don't meet the customized security necessities, in the mean time, it loses the opportunity to accomplish better utility by exploiting contrasts of clients' protection prerequisites.

This paper is roused by the distinguishment of the requirement for a better grain and more customized security in information production of informal communities. We propose a protection security conspire that not just keeps the divulgence of character of clients additionally the exposure of chose gimmicks in clients' profiles. An individual client can choose which gimmicks of her profile she wishes to hide. Properties of client are indicated either as delicate or as non-touchy. We give client more security alternatives and security by utilizing client data and criticism.

II. RELATED WORK

Yi Song Panagiotis Karras, Qian Xiao Stephane Bressan has explore the method to present privacy protection algorithms that allow for graph data to be published in a form such that an adversary who possesses information about a node's neighborhood cannot safely infer its identity and its sensitive labels.

Seda Gurses and Claudia Diaz has first provide an introduction to the surveillance and social privacy perspectives emphasizing the narratives that inform them, as well as their assumptions, goals and methods. They then just expose the differences between these two approaches in order to understand their complementarily, and to identify potential integration challenges as well as research questions that so far have been left unanswered.

Mingxuan Yuan Lei Chen Philip S. Yu has explore the method to They introduce a framework which provides privacy preserving services based on the user's personal privacy requests. Specifically, they define three levels of protection requirements based on the gradually increasing attacker's background knowledge and combine the label generalization protection and the structure protection techniques (i.e. adding noise edge or nodes) together to satisfy different users' protection requirements. They verify the effectiveness of the framework through extensive experiments.

Leucio Antonio Cutillo Refik Molva Thorsten Strufe Sophia Antipolice has developed the method to suggest a new approach to tackle these security and privacy problems with a special emphasis on the privacy of users with respect to the application provider in addition to the defense against intruders or malicious users. In order to assure users' privacy

in the face of potential privacy violations by the provider, the suggested approach adopts a decentralized architecture relying on the cooperation among a number of independent parties that are also the users of the on-line social network application. The second strong point of the suggested approach is to capitalize on the trust relationships that are part of social networks in real life in order to cope with the problem of building trusted and privacy preserving mechanisms as part of the on-line application. The combination of these design principles is Safe book.

Seda G¨urses and Claudia Diaz contend that these distinctive security issues are entrapped, and that OSN clients may advantage from a superior joining of the three methodologies. For instance, consider reconnaissance and social security issues. OSN suppliers have admittance to all the client created substance and the ability to choose who may have entry to which data. This may prompt social security issues, e.g., OSN suppliers may build content deceivability in sudden courses by overriding existing protection settings. In this way, various the security issues clients involvement with their "companions" may not be because they could call their own behavior, however rather come about because of the vital configuration changes actualized by the OSN supplier. If we concentrate on the protection issues that emerge from misinformed choices by clients, we may wind up deemphasizing the way that there is a focal element with the ability to focus the availability and utilization of dat.

III. PROPOSED SYSTEM

The research methodology to be employed as follows:

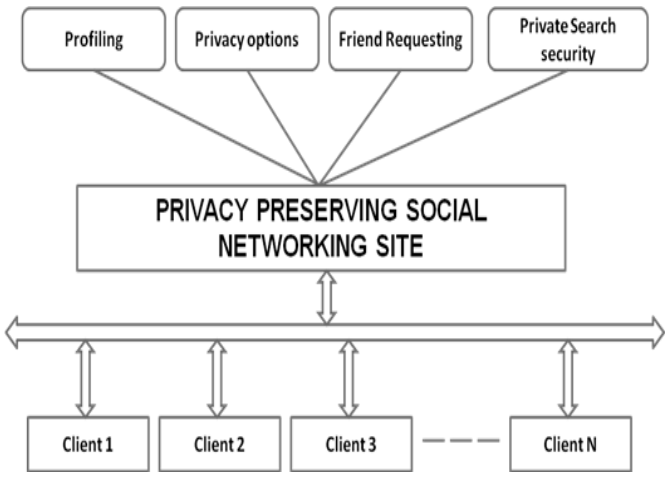

Fig. 1 : System Architecture

1. Authentication Module:

These modules basically consist of the user registration and login. Password is secured using MD-5 hash algorithm.

2. Role based login:

Normally, every user has its own role to play into the system but in this system there are two main roles i.e. admin and normal user. Admin will monitor the database usage while normal users can use it freely as any social network site.

3. Group Creation Services:

Whenever the user want to post a new notification or has to either select an existing group or create a new group to whom the notification will be limited. The new part in this project is that not only the notification is made private to group but all the notifications in it are also made private i.e. if anyone in the group comments on the post it will only be shown to group users.

4. Privacy Services:

The social networking sites today have only a few number of privacy options. For example, facebook gives only four options (i.e. only me, Friends, Friends of Friends, and Public). But in real life the friends group can again sub-divided into college friends, their colleagues and so on. Our scenario will help the user to choose among many different privacy options and again they can create their own privacy options for group.

5. Email Services for forgot Password:

This email service is used to send the temporary password to the user when he/she wants to use forgot password facility.

IV. EXPECTED OUTCOME

The output of the project will be shown in the real time scenario with the help of three or more systems where multiple users will be created with friends. The demonstration will be done by posting the notifications and then by using privacy and grouping options. The system will be able to improve security and privacy of user data in the system.

V. CONCLUSION

We have studied different literatures that are provided at the present. Our project covers some existing features and at the same time provides the many new privacy and security options for the users of social networking site. This project will help to the prevent data leakage of users in the social networking sites which occur due to poor privacy options with the help of strong privacy and security options.

REFERENCES

[1] Yi Song, Panagiotis Karras_, Qian Xiao, and St_ephane Bressan, “Sensitive Label Privacy

Protection on Social Network Data", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING VOL: 25 NO: 3 YEAR 2013.

[2] S. Bhagat, G. Cormode, B. Krishnamurthy, "Class-based graph anonymization for social network data." PVLDB, 2(1), 2009.

[3] Leucio Antonio Cutillo Refik Molva Thorsten Strufey Institute Eurécom Safe book: "Privacy Preserving Online Social Network Leveraging on Real-Life Trust" IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING VOL:25 NO:3 YEAR 2013.

[4] G. Cormode, D. Srivastava, T. Yu, and Q. Zhang." Anonym zings bipartite graph data using safe groupings". PVLDB, 19(1), Year 2010.

[5] Mingxuan Yuan, Lei Chen, and Philip S. Yu. "Personalized privacy protection in social networks."PVLDB, 4(2), Year 2012.

[6] Seda Gurses and Claudia Diaz, "Two tales of privacy in online social networks", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING VOL:25 NO:3 YEAR 2013

[7] Y. Song, P. Karras, Q. Xiao, and S. Bressan. Sensitive label privacy protection on social network data. Technical report TRD3/12, 2012.

[8] Y. Song, S. Nobari, X. Lu, P. Karras, and S. Bressan. On the privacy and utility of anonymized social networks. In iiWAS, pages 246{253, 2011.

[9] FTC. Ftc charges deceptive privacy practices in google's rollout of its buzz social network. Online, 03 2011.

[10] Glenn Greenwald. Hillary clinton and internet freedom. Salon (Online), 9. December 2011.

[11] James Grimmelmann. Saving facebook. Iowa Law Review, 94:1137– 1206, 2009.

[12] Kevin D. Haggerty and Richard V. Ericson. The Surveillant Assemblage. British Journal of Sociology, 51(4):605 – 622, 2000.

[13] Heather Richter Lipford, Jason Watson, Michael Whitney, Katherine Froiland, and Robert W. Reeder. Visual vs. Compact: A Comparison of Privacy Policy Interfaces. In Proceedings of the 28th international conference on Human factors in computing systems, CHI '10, pages 1111–1114, New York, NY, USA, 2010. ACM.

[14] Evgeny Morozov. Facebook and Twitter are just places revolutionaries go. The Guardian, 11. March 2011.

[15] Deirdre K. Mulligan and Jennifer King. Bridging the gap between privacy and design. Journal of Constitutional Law, 14(4):989 – 1034, 2012.

[16] Leysia Palen and Paul Dourish. Unpacking "privacy" for a networked world. In CHI '03, pages 129 – 136, 2003.

[17] Kate Raynes-Goldie. Privacy in the Age of Facebook: Discourse, Architecture, Consequences. PhD thesis, Curtin University, 2012.

[18] Rula Sayaf and Dave Clarke. Access control models for online social networks. In Social Network Engineering for Secure Web Data and Services. IGI - Global, (in print) 2012.