ISSN 2395-1621

Implementation on Semantic Approach Security Online Social Networks by using privacy, policy

[#1]Bhagyashri Dhawle, [#2]Prof. S. B. Rathod

[1]dhawlebhagyashri@gmail.com
[2]sbrathod.sae@sinhgad.edu

[#1]Department of Computer Engineering
[#2]Prof. Department of Computer Engineering

Savitribai Phule Pune University
SAOE, Pune.

ABSTRACT

Now days, internet or social is one of the most efficient and effective ways to communicate and sharing the information using the social networking sites like twitter, Facebook, etc. With multiple people connected through online social networking sites and due to the popularity of online social network sites, more people are concerning about their own privacy and policy. it has become an important issue OSN. In this paper we will study how the current privacy plays on social network sites, analyze how personal information is being attacked by internet and social network, and also we identified how the privacy become a risk and how to employ security awareness to avoid privacy risk.

Index term: privacy, social networks, security issues, OSN.

ARTICLE INFO

Article History

Received: 20th June 2017

Received in revised form :

20th June 2017

Accepted: 23rd June 2017

Published online :

23rd June 2017

I. INTRODUCTION

Online/Internet users use social networking website to communicate with attached with OS friends, share anything like, photos, and videos, etc. It's very critical for all internet computer users to be don't know anything about computer security and privacy and to know what steps to take to defend against attacks. Social networking privacy issues have risen among users. As number of social networks is growing, the default settings share everything and what is important is that users have to set their privacy setting options to make their accounts more private. At the same time security attacks continue to be a major concern of all users. How to keep computers and social networking more secure and more private are the challenges that have been concern for every users. Not only because of the number of attacks but also because of the difficulties faced in defending against these attacks and threats.

Online networks provide significant advantages both to the individuals and in business sectors. Many users provide information about themselves on social network which can be searched and hacked by the strangers. Thus, it raises privacy and security issues. Unfortunately many users are not aware of this.

Related Social Network:

The social network websites are used by the young user of this generation. Facebook application is the mostly used by the internet users. Users create user profile in OSN applications with and existing E-Mail id. Once the user profile is created, the users can post their real images, personal information such as E-Mail id, Phone numbers, and home address and so on. They can post their day to day activities, life style, what they like and don't like and even users are tagging their present location in online social media. This shows very clearly that all the information about the people is most probably publicly available in online social networking applications. [1]

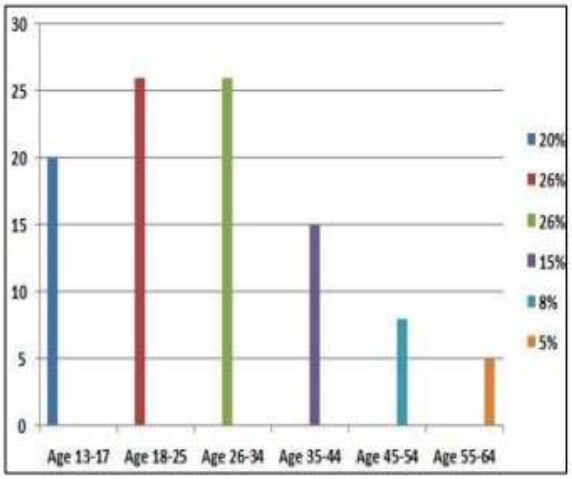

Figure 1 Online Social Network Users Age wise.

The Figure 1 shows the users of online social network applications age wise. From the Figure 2 it can be identified that people between the ages 18 to 34 are mostly using the online social networks. [1] In online social network applications all the people's sensitive information and their real images are publicly available.

II. REVIEW OF LITERATURE

Lewis, K., Kaufman, J., and Christakis, N.. (2008). Drawing upon a research based on Facebook, they argued that privacy behavior is an upshot of both social influences and personal incentives. Students are more likely to have a private profile if their friends and roommates have them; women are more likely to have private profiles than are men; having a private profile is associated with a higher level of online activity.

Debatin, Bernhard, Lovejoy, Jennette P., Horn, AnnKathrin, and Hughes, Brittany N. (2009). This research investigates Facebook users' awareness of privacy issues and perceived benefits and risks of utilizing Facebook. Research found that Facebook is deeply integrated in users' daily lives through specific routines and rituals. Users claimed to understand privacy issues, yet reported uploading large amounts of personal information.

Ai Ho Maiga, A. Aimeur, E. (2009). Their research examines the privacy protection issues on social networking sites (SNS) such as MySpace, Facebook and LinkedIn. Based on this study, they found that many users still are not aware of these threats and the privacy settings provided by SNS are not flexible enough to protect user data.

Boyd, danah, and Hargittai, Eszter. (2010). This research examines the privacy concerns voiced following the sense of exposure and invasion. In essence, the 'privacy trainwreck' that people experienced was the cost of social convergence.

Brady Robards. (2010). Their research on the Gold Coast, social network site in Australia argues that young users are consistent with developing increasingly complex strategies for managing their online privacy and social interactions.

Francesca Musiani. (2010). This research addresses and analyses the "first steps" of applications at the crossroads between social networks and P2P networks. More specifically, it discusses how such applications anticipate modifications in the management of users' right to privacy, by harnessing both anonymity and knowledge of identity – aspects generally identified with P2P networks and social networks, respectively – depending on the different functionalities and layers of the application.

Markus Huber, Martin Mulazzani, and Edgar R. Weippl. (2010). Within this research, they present novel friend injection attack which exploits the fact that the great majority of social networking sites fail to protect the communication between its users and their services. The friend injection attack enables a stealth infiltration of social networks and thus outlines the devastating consequences of active eavesdropping attacks against social networking.

Raynes-Goldie, Kate. (2010). This research explores how 20–something Facebook users understand and navigate privacy concerns. Based on a year–long ethnographic study in Toronto, Canada, this research looks at how — contrary to many mainstream accounts — younger users do indeed care about protecting and controlling their personal information. Boyd,

Danah, and Marwick, Alice. (2011). Based on the Facebook, the research found that both frequency and type of Facebook use as well as Internet skill are correlated with making modifications to privacy settings. In contrast, it also observe few gender differences in how young adults approach their Facebook privacy settings, which is notable given that gender differences exist in so many other domains online.

Fuchs, Christian. (2011). This research critisizes and introduces an alternative analytical framework for studying privacy on Facebook, social networking sites

and web 2.0. This framework is connecting the phenomenon of online privacy to the political economy of capitalism—a focus that has thus far been rather neglected in research.

Raynes-Goldie. (2011). Drawing on the existing body of primarily youth-focused research, particular focus is paid to the key debate around youth and privacy attitudes (the 'privacy paradox'), with an examination of newer research on adults and social network use.

III. RELATED WORK

Input: Image
Output: Privacy policy apply to image.

Algorithm steps:

Step 1: Upload images on sites

Step 2: Determine the value of the image according to the actual situation

Step 3: Calculate each input image value from user on server.

Step 4: According to the threshold value to assign policy to the uploaded images.

Step 5: According to the threshold value to assign privacy to the uploaded images.

Step 6: The rest of the cloud center point as input data of obtain K value.

Step 7: After the k value is determined, Choose I Image their assign security.

Step 8: According to the initial value, user access the image using the policy role.

Step 7: Calculating the average of all the data in each class as the new center.

Step 8: Repeat steps 6 and 7 until the objective function converges.

Step 9: User can set public and private policy to the uploaded image.

Step 10: Stop

Advantages:
1. It also prevents hacking.
2. It uses Encryption algorithm for image secure
3. The system prevents identity theft.
4. It also provides security to the user personal data.

IV. PROPOSED SYSTEM

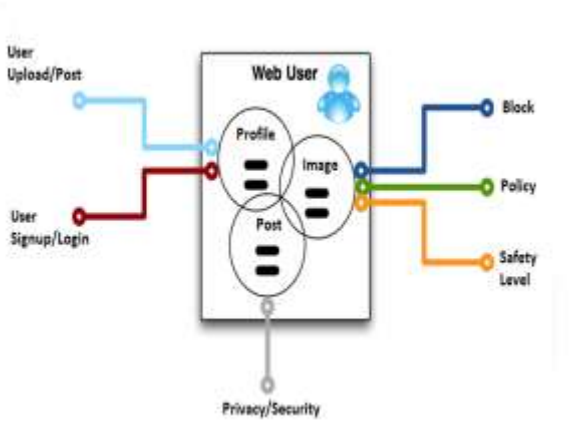

Fig 2. System architecture

The proposed system Secure Request-Response Application Architecture. It is an architecture developed for the secure data sharing on OSN websites. This architecture allows a user to accept or reject the request of accessing information from his profile. The user can reject the request of friend as well as the visitors. The second functionality of this architecture is that user can have two different databases with different information provided. The user may select data from any one of the two databases to response a particular request. This architecture improves the degree of customization of the profile of a user. According to this architecture the visitors or friends request for any information to the application between the visitor and the user. The application requests to the user for the response then the user can response from any one of the databases according to his trust on the person who has requested for the information.

Image security and checksum generation

Data user upload the images on social network, checksum on cloud after privacy apply.

Image Access via privacy access

Registered user access the images of the other users if particular user give the access privacy to the personal images.

Search Images

Registered user access the images of the other users, user search the images based on the keywords. If some keywords match then find the images basis on search keywords.

SOFTWARE REQUIREMENT SPECIFICATION

We have created system in java programing. Data is stored in mysql database. We have created a web

application with local server. Web application that communicates with local server and Trustee Server using REST API. We have uploaded image on cloud, add profile, post comment, apply security, privacy on online social network.

V. MATHEMATICLA MODEL

Our system can be represented as a set
System S = {I, O, C}
Where,
I=set of inputs
O=set of outputs
C = set of constraints
Input
Input I = {Login, Request}
Login = {Username, Password}
Request = {Upload images, Search images, download images, Apply security, View History}
Users = {User, Service provider}
Username = {Username1, Username2… Username n}
Password = {Password1, Password2… password n}
Output
Output O = {Display uploaded images, Download start, Prevent hacking, Display history}
Constraint
C = "User should login to the system

VI.RESULT

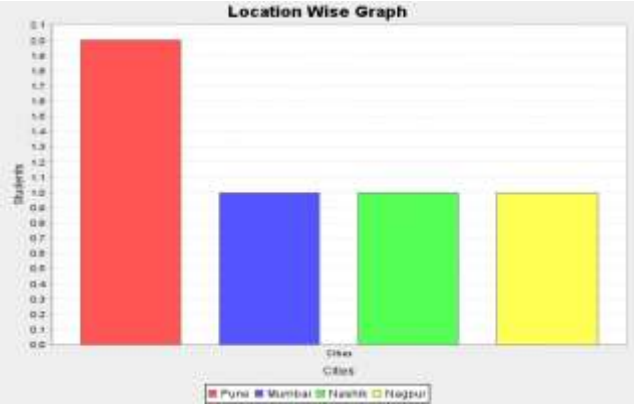

Fig 3. Here we analysis the location wise active users as well as performance result

VII. ACKNOWLEDGEMENT

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally I wish to thank to all our friends and well-wishers who supported us in completing this paper successfully I am especially grateful to our guide for time to time, very much needed, valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

VIII. CONCLUSION

This paper introduced a technology and social network have made interaction and communication much easier than early decade. In this paper, we have briefly come across privacy on social network. As many websites and social networks out there, people are more concern on how much privacy do they still have. We have also highlighted what is the current situation on using social network, as well as what are the threats that can affect the users on social network.

REFERENCE

[1] M. Milton Joe, Dr. B. Ramakrishnan, " A Survey of Various Security Issues in Online Social Networks, International Journal of Computer Networks and Applications Volume 1, Issue 1, 2014.

[2] Lewis, K., Kaufman, J., and Christakis, N.. (2008). The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. Journal of Computer-Mediated Communication, 14(1), 79-100. (journal article)

[3] Debatin, Bernhard, Lovejoy, Jennette P., Horn, Ann-Kathrin, and Hughes, Brittany N.. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. Journal of Computer-Mediated Communication, 15 (1), 83 - 108. (journal article)

[4] Ai Ho Maiga, A. Aimeur, E. (2009). Computer Systems and Applications, IEEE/ACS International Conference, AICCSA 2009. 271 – 278. (conference paper)

[5] boyd, danah, , and Hargittai, Eszter. (2010). Facebook Privacy Settings: Who Cares?. First Monday, 15 (8). (journal article)

[6] Brady Robards. (2010). Randoms in my bedroom: Negotiating privacy and unsolicited contact on social network sites. PRism, 7(3). (journal article)

[7] Francesca Musiani. (2010). When Social Links are Network Links: The Dawn of Peer-to-Peer Social Networks and Its Implications for Privacy. Observatorio (OBS*), 4 (3), 185-207. (journal article)

[8] Markus Huber, Martin Mulazzani, and Edgar R. Weippl. (2010). Who On Earth Is Mr. Cypher? Automated Friend Injection Attacks on Social Networking Sites. Security and Privacy--Silver Linings in the Cloud, 1, 80--89. http://friendinjection.nysos.net (journal article)

[9] Raynes-Goldie, Kate. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. First Monday, 15(1). (journal article)

[10] boyd, danah, and Marwick, Alice. (2011). Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies. Privacy Law Scholars Conference.Berkeley, CA May.

[11] Fuchs, Christian . (2011). An alternative view of privacy on Facebook. Information, 2 (1), 140-165. Special issue on "Trust and privacy in our networked world", edited by Dieter M. Arnold and Herman T. Tavani (journal article)

[12] Raynes-Goldie. (2011). Annotated bibliography: Digitally mediated surveillance, privacy and social network sites. (misc).

