A Survey of Semantic Approach to Detect Security issues in Online Social Networks

Shubhangi Dethe[1], Prof. Prashant Jawalkar [2]
[1, 2] Dept of Computer Engineering
[1, 2] JSPM BSIOTR, Wagholi, Pune

Abstract- *Now days, net or social websites is normally used inside the international and every other use identity one of the maximum efficient and powerful ways to speak and sharing the information the usage of the social networking websites like twitter, facebook, and many others. With more than one people are related to the net social networking sites and that's why the popularity of on line social network websites is greater in the global, additionally more people are concerning about their personal privateness and coverage. It has become an critical problem OSN. On this proposed machine we will study how the current privacy plays on social community websites, we also examine how non-public data is being attacked with the aid of internet and social network. We also recognized how the privateness turns into a danger issue and how to appoint protection awareness to keep away from privacy danger. We keep away from these kind of problems the usage of the encryption approach to the uploaded non-public snap shots.*

Keywords- OSN, privacy, security issues,social networks.

I. INTRODUCTION

The available online social networks sites are do not provide privacy and security to users. Their used centralized system structure and techniques employed for online information sharing has left wide holes for online attack, fraud, threatening users' lives. Therefore, we produced to ensure and enhance privacy structure and security architecture is needed that incorporates privacy principles and provides secure mechanisms for information sharing, communication, uploading toits users.

Online/Internet peoples use social networking website to sharing and communicate with attached with connected to OSfriends; share anything like, files, photos, and videos, etc. It's very risky and vital for all internet pc users to be don't understand something about computer safety and privateness and to recognize what steps to take to guard against assaults. Social networking problems have risen extra among related users. As range of social networks is every day developing makes use of, the default settings customers are percentage the whole lot on online socials websites.

What's vital in that case users have to set their privacy setting alternatives to make their money owed extra personal? On the identical time safety assaults stay a prime concern of all customers. We observe the way to preserve computers and social networking greater comfy and greater personal are the challenges which have been subject for every customers. Not simplest due to the wide variety of assaults however additionally because of the problems faced in defending towards those attacks and threats.

Online networks offer to the customers sizable benefits each to the individuals private use and in commercial enterprise sectors. many users provide information about themselves on social network which may be searched and hacked by means of the strangers. As a result, it increases privateness and protection problems. So lamentably many users are not aware about this all troubles and threads.

Related Social Network:

We study social network websites regarding evaluation which peoples are by and large connected we identified primarily young user of this generation. Now day's fb software is the typically utilized by the internet customers. Customers create user non-public profile in OSN packages with and current E-Mail identity. Once the user create profile on OSN then users have authority post their actual pix, non-public information consisting of e mail identification, cell numbers, and cope with and so on. They could put up their life fashion, everyday activities what they don't like and like and even customers are adding. tagging, likes their gift area in online social media. This primarily details shows very genuinely that each one the statistics approximately the related human beings and is most probable publicly to be had in online social networking packages. [1]

The below Figure 1 indicates the customers take a look at to be had online social community programs test active person exceptional social networking sites. From the Figure 1 it may be identified which that human beings are usually using the net social networks. [1] In online social community packages all of the connected people's, touchy information and their real photos are publicly to be had.
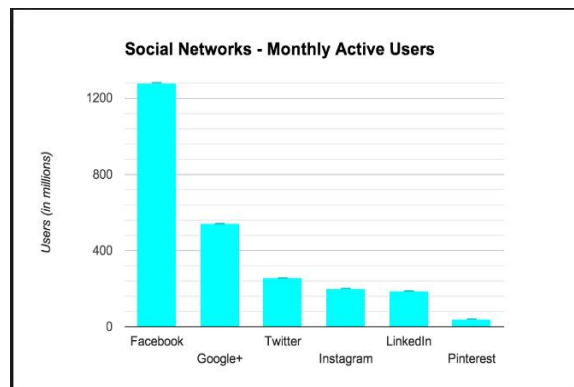
Figure 1 Online Social Network Users active.

II. REVIEW OF LITERATURE

Lewis, K., Kaufman, J., and Christakis, N.. (2008).In this paper writer, look at upon a studies based on fb, they argued that privateness conduct is an upshot of both social impacts and private incentives. Creator's scenario students/peoples are much more likely to have a personal profile if their pals and roommates have them; author scenario girls are much more likely to have personal profiles than are guys; in the OSN having a personal profile is associated with a better level of online pastime.

AnnKathrin,Debatin, Bernhard, and Hughes, Brittany N. (2009). This research author investigates social networking web sites on fb users' awareness of privacy issues and perceived benefits and dangers of making use of fb. in that studies located to the author that facebook is deeply incorporated in users' each day lives through unique routines and rituals. Users claimed to understand privateness problems, but said importing massive quantities of personal information.

A.Aimeur (2009).Their studies studies the privateness protection issues on social networking web sites (SNS) extra crucial consisting of MySpace, Facebook and Linkedin. Based totally on this research, creator found that many users nevertheless are not privy to these threats and the privateness settings supplied through SNS are not bendy enough to defend person statistics on online social community.

Hargittai, Eszter and Boyd, danah, (2010). On this research paper writer examines the privacy issues voiced following the sense of publicity and invasion. In essence, the 'privateness educate spoil' that human beings skilled changed into the value of social convergence.

Edgar R. Weippl,Markus Huber, (2010). On this studies author defend the assaults, they gift injection assault on social community websites which exploits the truth that the high-quality majority of social networking websites fail to defend the conversation between its customers and their offerings. The injection attack turns on a stealth infiltration of social networks and as a result outlines the devastating outcomes of active eavesdropping assaults in opposition to social networking.
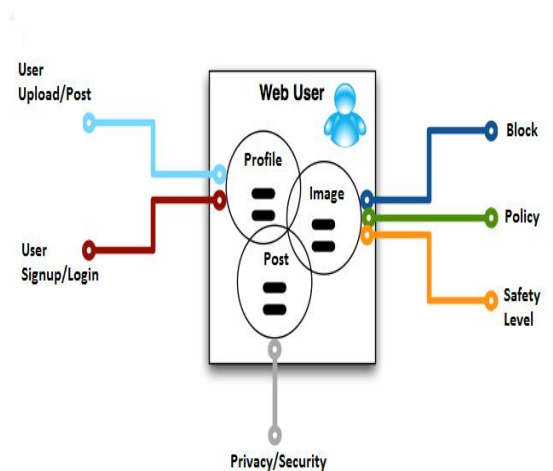
III. SYSTEM OVERVIEW

Fig 1. System architecture

In this proposed system we secure request-response Application Architecture implemented. Proposed architecture developed for the secure data sharing to the connected on OSN websites. This structure permits a user to simply accept or reject using the privacy policy putting the request of gaining access to records from his profile. The person cans additionally authority to simply accept and reject the request of pal as well as the visitors. The second one functionality we implemented of this proposed structure is that person can have two extraordinary database used to get entry to with distinctive records supplied to the users. The consumer might also pick out information from anybody of the two databases to response a particular request. This gadget architecture improves the degree of customization of the profile of a consumer using the blockading method. In line with this system architecture the visitors and pals request for any data to the utility server between the traveler and the person. The software requests to the person for the reaction then the consumer can response from any person of the databases consistent with his agree with on the person that has requested for the information.

IV. 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. ALGORITHM

Algorithm:

Input: Image
Output: Privacy policy applies to image.

Algorithm steps:

Step 1: Upload images on sites
Step 2: Decide the price of the picture in keeping with the actual state of affairs.
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 relaxation of the cloud middle point as input records of achieve k cost.
Step 7: After the k value is determined, Choose I photo their assign security.
Step 8:According to the initial value, user access the image using the policy role.
Step 9: Calculating the average of all the information in every class as the brand new middle.
Step 10: Repeat steps 6 and 7 till the objective feature converges.
Step 11: User can set public and private policy to the uploaded image.
Step 12: Stop

VI. SYSTEM ANALYSIS

Security risks

In this security danger OSN sites growing uses so risk factor additionally increases. We have a look at some of the security dangers are identity robbery, phishing, and so forth. humans use OSN to provide their personal data on SNSs like fb, twitter etc. this facts is saved in SNS and in loss of right security techniques carried out in SNSs, it is not comfortable to the customers.

Phishing

Phishing attack is the manifest broadly in SNS began in 2007[3]. The usage of phishing is to harm economically that is the phishers try to retrieve the profile statistics to recognize approximately the banking or the financial statistics of the users. Once person login phish internet site then attacker get all statistics from the users.

Identity Theft

Attackers assault through the online social utility wherein they asking permission for accessing the information supplied within the profile of SNS. While a person offers permission to achieve this, they get all of the statistics and might misuse that without difficulty without the person know-how or permissions.

Profiling Risk

Profiling threat is the risk related to profile cloning. the attackers retrieve the personal information of the users and make a clone of the profile [2]. They accomplish that to make their social photo bad or for different purposes like understanding approximately buddies of sufferers. This is the maximum famous security hazard associated with the SNSs due to the fact it's far very clean to do without the permission of the person.There is almost no safety for profile cloning in SNSs.

VII. RESULT

We propose a sensitive policy; privacy based approach for the content sharing networks model.

- For minimizing the loss of the uploaded images from unauthorized user .
- For minimizing the disclosure risk.
- To maintain the diversity among the uploaded images.
- Minimized security risks on images on sharing sites.

VIII. CONCLUSION

This paper we brought a brand new generation and social network have made interaction and communique plenty simpler than early decade. In this paper, we've in short have a look at throughout privacy policy on social network. As many web sites and social networks, people are greater difficulty on how lots privateness do they nevertheless have. We've also highlighted current state of affairs on the use of social community, as well as what are the threats and troubles which could have an effect on the customers on social community.

IX. ACKNOWLEDGMENT

REFERENCES

[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).