www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 3 March 2015, Page No. 10799-10803

A Social Chat Network Site With User Anonymity Consideration

Oyinloye O.Elohor, Akinyemi B.Peter

ABSTRACT
Preserving privacy in social networks against neighborhood attacks is an initiation which uses the definition of privacy called K-anonymity. K-anonymous social network still may leak privacy under the cases of homogeneity and background knowledge attacks. To overcome, we find a place to use a new practical and efficient definition of privacy called G-anonymity. In this paper, we take a step further on preserving privacy in collaborative social network site by developing a site using the G-anonymity to improved user privacy on the social media for unaware and illiterate users. Testing was performed using five users and from the users comment; it was observed that the system is 70% efficient for their usage which is better than the other existing systems.

KEYWORDS:Social-network site, K-anonymity, privacy, neighbourhood attacks, G-anonymity

Social networking service is an online service, platform, or site that focuses on facilitating the building of social networks or social relations among people who, for example, share interests, activities, backgrounds, or real-life connections. A social network service consists of a representation of each user (often a profile), his/her social links, and a variety of additional services. Most social network services are web-based and provide means for users to interact over the internet, such as e-mail and instant messaging **[1]**. Online community services are sometimes considered as a social network service, though in a broader sense, social network service usually means an individual-centered service whereas online community services are group-centered. Social networking sites allow users to share ideas, activities, events, and interests within their individual networks. Social network is a social structure made up of a set of actors (such as individuals or organizations) and the dyadic ties between these actors. The social network perspective provides a clear way of analyzing the structure of whole social entities. Study of these structures uses social network analysis to identify local and global patterns, locate influential entities, and examine network dynamics **[1]**. What makes social network sites unique are because that they enable users to articulate and make visible their social networks. This can result in connections between individuals that would not otherwise be made, but that is often not the goal, and these meetings are frequently between latent ties **[2]** who share some offline connection. On many of the large social networking site, participants are not necessarily networking or looking to meet new people; instead, they are primarily communicating with people who are already a part of their extended social network. To emphasize this articulated social network as a critical organizing feature of these sites, they are label led social network sites. When people join social networking sites, they begin by creating a profile, then make connections to existing friends as well as those they meet through the site. A profile is a list of identifying information. It can include your real name, or a pseudonym. It also can include photographs, birthday, hometown, religion, ethnicity, and personal interest. Members connect to others by sending a "friend" message, which must be accepted by the other party in order to establish a link. Another member gives them access to your profile, adds them to your social network, and vice versa. Members use these sites for a number of purposes. The root motivation is communication and maintaining relationships. As there is a brisk growth of users using this social networking, the major issue that comes into play is security. The security issues that primarily considered are password protection, protection for the user private data and the privacy of the user. These security issues are not only the primary concerns of the users and the owners of the social networking, but also provide the wide scope to hackers if these security issues are not properly taken care of, some other problems faced with social networks include; social network sites are faced with many problems, such as;

Plug-in: Some applications on social networks prompt user to install some plug-ins like flash. The flaws in the plug-ins are threat to personal information.

Phishing: In this attack, attacker pretends like a legitimate user and sends requests to the other users by using phishing, which gains access to others personal information on their acceptance to the request.
Viral Marketing: Attackers makes use of weakness of users to receive advertisements from friends. The attackers make the marketing malware functions through attracting videos or advertisements. The only investment for the attackers is marketing the videos or advertisements.
Spam: Earlier spam spread by using email, which spreads through social networks. Spam damages the network by residing at the computer. Spam mainly spreads through advertisements with help of friend list on the social network.
Third party applications: Flaws and security features in the third party applications are the major areas through which attackers can get access to the social networks. As number of applications increases, more number of flaws increases there by resulting in loss of data.
Worm: Worms will replicate themselves automatically by their self-replicate nature. Worms are specialized in stealing the personal information like password, bank account number.etc
And this may affect lots of users within a short period of time, since each user is regarded as a trusted user. And this research is requiring making sure that:
* Confidentiality, integrity, and availability of user data. That means, data should be hidden from unauthorized parties, and intended users should be able to access and verify the integrity of the latest copy of a piece of data.

* Data owners should be able to have complete control over the permissions to the content they create and no user should be able to access content unless explicitly authorized by the owner.
* Relationships are also considered private information and should be hidden from unauthorized parties.
. In this paper we discussed design of an enhanced social network site with improved user privacy.

RELATED WORKS
Several attacks exist that are common to most existing social sites,they include; account cross-site scripting (xss) , cross-site request forgery (csrf), de-anonymize attack & neighborhood attack in **[7**].

FACEBOOK
Is global social networking website that is operated and privately owned by Facebook, Inc. Facebook provides user with variety of options to maintain the contacts with friends loved ones and even with different people in the society. The options include adding friends sending public and private messages to friends, updating profile **[3] .**Hackers now focus on it because it is highly accepted in most countries, and the facebook owner has worked extensively in other to stop the hackers from hacking his network, where he has used some security measure to stop them which is unknown to people except their own teams.

MYSPACE
Is one of the leading social networking websites. MySpace became the most popular social networking site in the United States in June 2006. The very first MySpace users were eUniverse employees. MySpace redesigned many of the features of its site in both layout and in function. One of the first functions to be redesigned was the user home page, with features such as status updates, applications, and subscriptions being added in order to compete with Facebook. In 2008, MySpace homepage was redesigned. MySpace Music was recreated in fall of 2008 along with an updated version of MySpace profile. Myspace has a groups feature, which allows a group of users to share a common Page and message board. Groups can be created by anybody, and the moderator of The group can choose for anyone to join, or to approve or deny requests to join. In Early 2006, myspace introduced myspace, an instant messenger that uses One's myspace account as a screen name. Myspace user logs in to the client using the same e-mail associated with his or her myspace account. Unlike other parts of Myspace, myspace is stand-alone software for Microsoft windows. Users who use myspace get instant notification of new myspace messages, friend Requests, and comments **[4].** And due to their popularity hackers focus them by hacking their users using attacking techniques such as Koobface attack, Image attack, Structure query language injection attack, User anonymity attacks. Etc
ORKUT
On January 24th 2004 Google launched a revolutionary free-access social network called Orkut, to help the people in maintaining relationship with friends and loved ones. Orkut is named after google employee Orkut Buyukkokten, who is the founder of Orkut, it provides the user with adding new friends and communities to his/her profile. Along with features, Orkut also provides the user with additional space to upload photos and videos to their profiles [**5] .**
Security threats on this site are as follows: XSS cross site scripting, Spam phishing attack, Spoofed email attack, User anonymity attack. Etc
TWITTER

Is the one of the most commonly used social networking services and it also falls under micro logging service, that was developed and maintained by twitter inc. according to the recent survey, about 65 million tweets are posted each day, which is equivalent to about 750 tweet sent each second. The basic mechanism in this social networking site is to send and view the message posted by different users, these

message in this networking site are known as tweets, and the maximum length allowed to be entered and posted on a single tweet is 140 characters and the format is the text based, and these message are displayed on the account owner page. But security is one of the prime concerns of the twitter; twitter collects the personal data entered by the user of the account and gives them to the third party for its usage [6**]**.

Security threat of the site are Spoofing attack, Worm infects, Denial of service attacks' User anonymity attacks. EtcBLACKBERRY MESSENGER (BBM):

Blackberry messenger is a mobile proprietary internet-based pin instant messenger and video telephony application included on blackberry devices that allow messaging and voice calls between blackberry and android users. Blackberry messenger are sent over the internet and use the blackberry pin system. The services communicate over the phone internet connection using the mobile phone network. A wireless LAN network connected to the internet may also e used to send messages , most service providers allows sign-in to Bbm if you have a blackberry data plan which are not needed for blackberry10, and androids. Bbm also allows e-mail and other data transmission (including pin-to-pin internet browsing and other voice data services messages) to be sent over the air.

Security threat on blackberry messenger:

1) Malwares
2) Loss and theft
3) Data communication interception
4) Direct attacks by pin
5) User anonymity attack. Etc

And after accessing all the existing social networking sites, I was observed that they are all suffering from user anonymity attacks, which gives the attackers the opportunity to hacks their users. But Bbm is suffering from those security threat because is a mobile proprietary internet-based pin instant messengers, except from anonymize attack which is the security measure that will employed, Then using some security measure of Bbm and k-anonymity which is the security measure of user anonymity attacks to develop the proposed social networking site.

The existing systems are suffering from de-anonymize attacks which occurs in two ways, first, the attacker will obtain group membership information from the social network. That is, the attacker has to learn, for some (possibly many) groups, who the members of these groups are before hacking. In the second way, the attacker uses history stealing to check the victim's browser for Uniform Resource Locator (URL).

THE DESIGNED SYSTEM

Figure 1 illustrates the logical connections between the components of our proposed system. The user interface is presented to the user through a browser, and it directly connects to the Layout Engine as needed. It is also connected to the Social Networking module, which provides the social networking functionalities. The data is stored in a Database, which the structure query language periodically queries to analyze all available data. The Social Networking module will maintain a Social Graph of all user relationships and interactions.

THECLIENT/SERVER ARCHITECTURE OF THE SYSTEM

The software architecture for the client-side Web UI software consists mainly of JavaScript model classes used to represent the locations of elements on the page. Objects of these classes are saved to the database through requests to the web server or instantiated from saved object states retrieved from the web server. The software architecture for the server-side software consists mainly of controllers and models. It uses Model View Controller architecture. Controllers use instances of Models and Views to render a page for the user. Requests are mapped to member functions of controllers based mainly on the request URI and HTTP method. The natural language processor is implemented as a client-server system as well. The NLP server is responsible for the language processing functionalities of the system. It uses TCP functionalities to receive communications from the NLP client. It also interfaces directly with the database to fetch information independently of the rest of the system. Figure 1 Show the connection between the home page phase, the sign up page phase, and the server application phase with the relationship between the

IMPLEMENTATION OF THE SYSTEM

The images in figure 2 to figure 5 below show a summary of the system upon implementation:

Figure 2

Figure 4

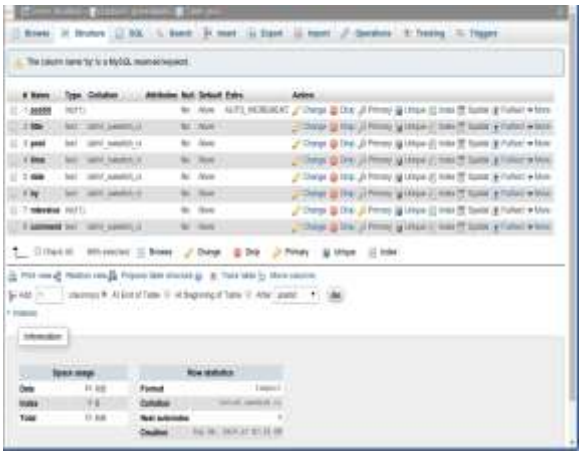

Figure 5

Username Used	Assigning a value of 1-5 rate the system on ease of use	Assigning a value of 1-5 rate the system on Application Responsiveness, speed and Flow	Time Used Exploring the Application (minutes)	Assigning a value of 1-10 give the Overall Rating of the Web Application	Comment
434567AD	3	3	20	7	The ability to rate positively and negatively with values from -5 to 5 is incredible
323456DE	3	4	20	6	The background of the site is good and enticing.
678907SF	4	4	15	5	Opportunity giving to the users to download books from the site is excellent but can we trust this application.
453678PZ	4	4	30	8	Why should I use pin to login and not my email address.
567893GH	2	3	45	6	Showing real name of the commented user and not their UserId is marvelous.

EXPERIMENTAL DISCUSSION

The system was tested using five users as shown in the table below.

All users confirmed the acceptability of the design as well as the flexibility of the system. In the course of the testing the users were presented systems to create account and view each other's profile. The users confirmed further that the ability of the system to secure their profile was of great value as most users of social networks have little knowledge the poor security of their privacy

Username Used	Assigning a value of 1-5 rate the system on ease of use	Assigning a value of 1-5 rate the system on Application Responsiveness, speed and Flow	Time Used Exploring the Application (minutes)	Assigning a value of 1-10 give the Overall Rating of the Web Application	Comment
434567AD	3	3	20	7	The ability to rate positively and negatively with values from -5 to 5 is incredible
323456DE	3	4	20	6	The background of the site is good and enticing.
678907SF	4	4	15	5	Opportunity giving to the users to download books from the site is excellent but can we trust this application.
453678PZ	4	4	30	8	Why should I use pin to login and not my email address.
567893GH	2	3	45	6	Showing real name of the commented user and not their UserId is marvelous.

RECOMMENDATION AND FUTURE WORK

This application will perform effectively for the intended purpose. This research has not outrightly concerned itself in the security of the database even thou the SHA algorithm was used to encrypt the content of the database, but better security techniques could be proposed for securing the database. Furthermore, a more convenient user password system can be proposed to improve the comfort of the user as well as the authentication parameter

REFEENCES

1 Boyd, D and Ellison, N. (2008). "Social network sites: definition," 13 journal of computer-mediated communications. PP: 1. Retrieved on may 14th,2013.

2 Haythornthwaite (2005) "Social network structures and uniqueness,"12th journal on computer- mediated communications. PP: 1. Retrieved on 25th of April 2014.

3 Facebook 2009, Available from www.facebook.com. PP: 24. Retrieved on Sept. 18th, 2014

4 Myspace 2009, Available from www.myspace.com. PP: 26. Retrieved on Sept. 2, 2014.

5 Orkut 2009, Available from www.orkut.com. PP: 26. Retrieved on March. 10th, 2014).

6 Prince Brian 2009, "Twitter DDoS Attack Takes Twists and Turns", eWEEK, Retrieved August 8, 2014.

7.Narayanan A and Shmatikov, V. 2009)"De-anonymizing social networks," in IEEE Symposium Security and Privacy, PP: 14. Retrieved on November 12, 2013.