Secure Framework for Social Networks

Chandan, Rajesh Jayaswar, Jayanti Arora, Rishi Raj Srivastava, and Bhawana Srivastava

***Abstract*—An Online Social Networking Site (OSNS) provides an easy way of interacting and sharing information with internet users across the globe. More than Millions of internet users have shared their personal and professional information publically over internet through these websites. On one hand these OSNS facilitate social interaction among the users while on the other hand it also introduce vulnerabilities like privacy invasion, identity theft and exposure of personal data such as photos, videos, email id, phone no. etc. to the other users on the network. This personal information available on the OSNSs can be misused by the attackers to perform malicious activities. The paper suggests architecture for improving privacy of any OSNS. Also a model is proposed that provide measures to protect users' personal data from the attackers as well as service provider of OSNSs. The proposed model has incorporated the concept of public and private key cryptography for data encryption, key distribution and management which helps to eliminate the concept of third party, which can be a potential point of attack. Finally, the concept of Safe-Space as a secure and reliable model of OSNS from privacy point of view has been introduced to protect users on OSNS.**

***Index terms*—Privacy, online social networking Sites, privacy framework.**

I. Introduction

In the previous and present decade the emergence and existence of social networking site like FaceBook, MySpace, LinkedIn, and Orkut, cannot be denied.

Users of different age groups, backgrounds, nationalities and with different level of skill are using these social networking sites. Millions of users publish their personal information and about their day-to-day activity on these sites. These online social networking site (OSNS) and applications severely suffer from various security and privacy exposures. The main reason behind the increase in popularity of these OSNS and usage of these services among the masses is the ease of sharing information with others, for either professional or personal purposes.

a) An Online Social Networking Sites (OSNS) can be defined as web-based services that provide users with functionalities to:
b) Create a public or semi-public profile with information related to a particular individual.
c) Create connections with other users and construct a list of other users with whom they interact
d) Share information among connected users.

There are more than hundred's of social networking sites [1] popular in various regions. Among which FaceBook, MySpace, Twitter and Linked in are few most famous ones.

Manuscript received May 20, 2011.

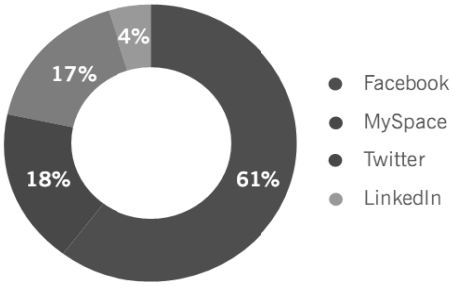

Figure 1: Social Networking Sites

There are more than 500 million active users on FaceBook [2]; 175 million on Twitter [3] and 375 million on MySpace [4].People spend over 700 billion minutes per month on FaceBook [5] and there are 95 million tweets on twitter per day. As stated in a report by Nielsen [6], web users in the United States have tripled the amount of time they spent on social networks in August 2009 compared to one year ago. According to Sophos' [7] survey of 500 organisations, revealed that cyber **criminals** have targeted 57% of users of social networking sites with spam and 36% with malware in the past year. Since personal information is involved in profile creating, therefore security protection of private information on OSNS has become a serious and important concern because social networking sites are gaining unprecedented popularity.

The main concern arouse from emergence of OSNS is the amount of information that user share on these site. Many individual behind the organizational networks tend to use these OSNS making organization's network prone to information loss. Social networking sites are ideal heaven for online criminal activities as they provide a combination of two key factors: a huge number of users and a high-level of trust among these users [8].

After going through, various solutions we found that the kind of privacy protection technologies that can effectively thwart the threats raised by user unawareness and server-side vulnerabilities is a client-side architecture that automates the process of privacy protection.

We have proposed an architecture, in which user data is kept on the server in encrypted form. Data is encrypted by using users' master key, which is unique to every user and is transferred between various users using public key cryptography. This provides a better key management scheme. Here one user encrypts his master key with another users' public key. Whereas second user using his private key to retrieve the original master key to decrypt the data. In our architecture, there is no involvement of any third party servers, which provides another dimension of security to our architecture.

Rest of the paper is organized as following: section 2 defines related work, section 3 is problem statement, section 4 describes Safe-Space architecture, and section 5 elaborate

the conclusions and future work.

II. Related Work

The privacy and security aspects of current OSNS have been analyzed and different solution has been given which involves the combination of cryptographic techniques along with the distributed techniques

Face Cloak [9], a model suggested for privacy in earlier research suggests storing fake profile for all users to prevent users' actual information from adversaries. This can be implemented using a third party server which itself introduces another point of compromise. Safe-space does not involve any third party server.

Face Cloak maintains two databases, one for storing users' actual data and second one for fake data that Face Cloak shows to all other users. This creates redundant storage. However, Safe-space does not involve any redundant storage.

Towards a Privacy-enhanced Social Networking Site [10] do not provide any key management solution. However, Safe-space does provide an efficient key management system.

In Face Cloak it is not possible to search any individual based on his profile details as all the provide details are fake. Also, the work done in the research model Hello word [11] is based on the concept of decentralization which makes searching any person a slow task. Safe-space comprises of two databases: plain and encrypted. Plain database consists of only that information sufficient for searching. Thus, this makes searching faster and efficient and also our encrypted information is secure.

III. Problem Statement

The issues considered in the papers ate to identify various privacy issues and weaknesses in the design of Social Networking Sites and to develop a new model to provide a more secure architecture for OSNSs. Protecting the privacy of users on OSNS is a complicated research task. No privacy protection model has been broadly accepted until now. Our aim is to protect privacy of a user from both OSNS administrator and from adversary.

IV. Proposed Solution

First we are listing the facts and assumptions considered in the proposed solution. Following are the facts considered about OSNS:

Privacy *Levels for OSNS:* Safe-Space is based on the concept of privacy levels explained in figure 2. In particular, there are three privacy levels. The three levels are Primary level, Secondary level and Tertiary level. The friends added in any user's account are classified among these three levels on the basis of the intimacy they have with the user.

There are three parameters, which differs with these three privacy levels. The three parameters are Degree, Friend type, Data. Apart from these three levels, there is also a visitor group, which comprises of the users not added in the user's account. This framework provides users with an easy and flexible way to specify and communicate their privacy concerns to other users and OSNS service provider. Based on the privacy level the user chooses, the user determines how much and which particular information user wants to share with that particular friend. The degree with respect to primary, secondary and tertiary level is 1, 2 and 3 respectively. The friends under the primary level are the best friends, Friends under the secondary level are the normal friends and the friends under the tertiary level are the casual friends. Coming to the data field, the users under degree 1 i.e. primary level are the best friends and therefore can share all the information like photos, videos, music, personal information etc. The friends who are assigned secondary level i.e. degree 2 are the normal friends. Therefore, they are given access to lesser information as compared to the friends of degree 1 like they are granted access to only a few photos out of the whole collection of photos. The rest of the photos might be personal to the user and the user might not want to share them with that particular friend. The friends under the degree 3 are the casual friends and hence they have limited access only, less than secondary level friends. The visitor group can only search their friends from the open or plain database and hence can see only the profile picture, full name and email-id of the person whom they are searching.

Following assumptions are very important for solutions which can be proposed for the problem assumed in the paper. Here we are assuming that users system is secure and OSNS (online social networking site) administrator is not trusted:

A. User System Is Secure: We assume that users' systems are not compromised. Here, we are completely relying on the integrity of users' web browsers, since our solution is put into action using a browser extension. The paramount security measures to ease this threat are to educate users to persistently patch browser vulnerabilities and install anti-virus software.

B. OSNS is not Trusted: A social networking site, can deliberately, reveal a user's personal information to parties not authorized by the user. However, an employee who is an authorized to access the database can break into the social networking site and can gain access to any user's personal information. Using these assumptions, we aim at making a solution, which is immediately usable and feasible also. We are proposing our model to protect user's privacy on social networking sites.、

PARAMATER	PRIMARY	SECONDARY	TRETIARY
DEGREE	1	2	3
FRIEND TYPE	Best friend	Normal friend	Casual friend
DATA	Full access	Less than primary	Less than secondary

Figure 2: Privacy Levels for OSNS

V. Safe-Space Architecture

A. Architecture

SAFE-SPACE architecture is proposed to enhance security of private data and availability of public data. Overall architecture of SAFE-SPACE is represented in

figure 7. Here the architecture employs both symmetric and asymmetric encryption techniques. It broadly comprises of two components

B. Safe-Space Server

1. Plain Database
2. Encrypted Database
3. Access List
4. Public Key Register
5. Encrypted Key Register

C. Client System

a) Client Module

Plain Database: This database contains non-sensitive information related to user like his name, profile image etc. which is accessible to all users. This database is useful for searching and making new connections.

Encryption Database: this database contains all other data and information that user wants to protect from unauthorized users, for instance personal images, videos and music etc. this database is encrypted using symmetric encryption technique.

Access List: Another component, which is being used in the proposed architecture, is the Access List. For each of the user on Safe-Space, an access list is created. The access list constitutes of three attributes tuple: <No., ID and level>. No. attribute is the serial number of a given row. ID attribute is the user identifier. Level attribute is to tell that at which level that particular friend is. i.e., in figure 3 we have created an access list of user A. Here we can see that B_ID, C_ID etc. are A's friend with different privacy levels.

NO.	ID	LEVEL
1.	B_ID	2
2.	C_ID	3
3.	D_ID	3
4.	E_ID	1
5.	F_ID	2
•	•	•
•	•	•
•	•	•

Figure 3: Access List of User A

Public Key Register: Safe-Space maintains a public key register, which contains the user ids and respective public key of each user on Safe-Space. This public key is used by users to encrypt their *master key* which is then stored in encrypted key register.

ID	PK
A_ID	PUB_A
B_ID	PUB_B
C_ID	PUB_C
D_ID	PUB_D
•	•
•	•
	•

Figure 4: Public Key Register

Encrypted Key Register: Safe-Space maintains a separate register for each user profile, which contains the user ids of its connections, and related key, which is formed by encrypting master key of that user with the public keys of respective connection. E.g. MEAB , is A's master key encrypted with B's public key.

ID	MEK
B_ID	ME_{AB}
C_ID	ME_{AC}
D_ID	ME_{AD}
E_ID	ME_{AE}
•	•
•	•
•	•

Figure 5: Encrypted Key Register of User A

Here in figure 5, which shows encrypted key register for A, contains user ids of its connections or friends and their respective decryption keys. This key is formed by encrypting A's master key with the public key of B for creating key for B. Similarly keys for C, D and E are created by encrypting A's master key with their respective public keys.

Client Module: Client Module is implemented on the user's computer as a web browser extension. It serves as the intermediary between the user and the Safe-Space server. It consists of three components: Encryption/Decryption, client access controller, interface and key manager.

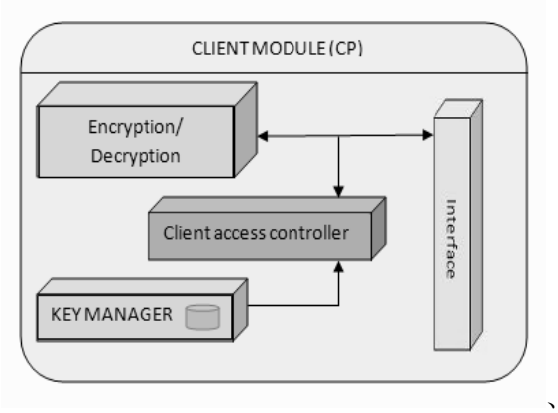

Figure 6: Client Module

Client Access Controller: It interacts with the Safe-Space and retrieves data that the user is authorized to access and forward it to encryption /decryption module or key management module.

Encryption/Decryption Component: This component performs the encryption of the data of the user and the decryption of the data, which is provided by the safe-space server.

Key Manager: key manager is component that stores and manages users' private key and its master key, which is used to encrypt and decrypt its own data.

Interface component: This is the component that retrieves the results from decryption module presents it to the user.

Processes Involved: We are taking a scenario where user A, B, C, D and E join Safe-Space by registering and creating their profile. When the user A registers at Safe-Space, a pair of Public and Private Keys (PUB_A, PRI_A) are generated for the user A. This private key PRI_A is stored in the Client side and the public key PUB_A is sent to the Safe-Space Public key Register *(Figure 4)*. Similarly, Public and Private Keys are generated for all registering users, their respective public keys are stored in the Public key register, and their private keys are Stored at Client side.

Every user generates a master key, which is used to encrypt its data and used by other users to decrypt the data. This key is stored at the user system by the key manager in the client module.

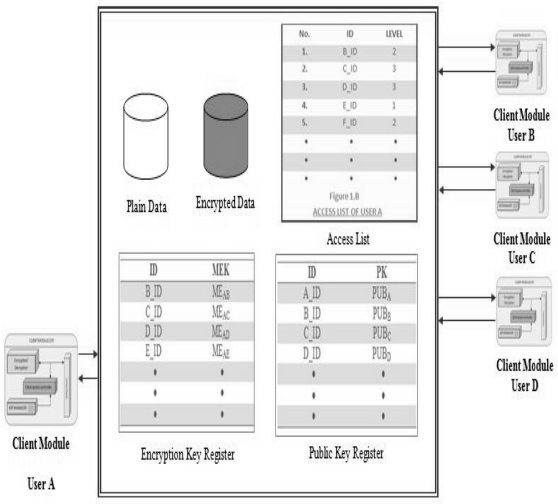

Figure 7
SAFE-BOOK SERVER

For all the users who access safe-space a client module (CM) is installed on user's system as an extension to its browser if it is not already installed on that system. CM works as a plug-in in client's browser which facilitates encryption, decryption and key management on client machine.

Suppose user A creates his profile on safe-space then Access List and Encrypted Key Register (EKR) are created for user A. His public key (PUB_A) is stored in Public Key Register (PKR). User A uploads his encrypted data using client module. When User B is added to user A then user B is added to access list of A and using user B public key from PKR user A encrypts master key of its own and stores it to EKR of user A. Now when the user B wants to access the profile of user A then he has granted permission using the access list of user A and his privacy level is checked. User B can access data only according to his permitted level. After this, using the private key of user B he will decrypt encrypted key (ME_{AB})and get master key of user A by which he will decrypt user A's data.

VI. Conclusions and Future Work

The paper discusses apparently secure architecture for an OSNS - online social networking site. These social networking sites provide ease of socializing with known and unknown people around the world. User profiles on these sites contain users' private information like his or her contacts, images, e-mail ids, etc. which can be misused by either any malicious attacker or even by the owner of the site. Thus our approach ensures privacy of his data by storing the data in encrypted form using symmetric encryption and sharing this key used for this encryption with other users by encrypting the key with public key of other users. For any application key management and distribution is an important component, thus improvements in this area would be a very valuable future work. More work is to be done in implementing the architecture. We aim to make our key management process simpler and also aim at automating the process of plug-in so that there is minimal involvement of the user for privacy concerns.

References

[1] List of social networking websites [online], http://en.wikipedia.org/wiki/List_of_social_networking_sites [Accessed 30 December 2010].

[2] M. Zuckerberg, "500 Million Stories," The Facebook Blog Wednesday, July 21, 2010. http://blog.facebook.com/blog.php?post=409753352130___[Accessed December 31, 2010].

[3] Twitter is the best way to discover what's new in your world. [Online],http://twitter.com/about [Accessed December 31, 2010].

[4] My Space social Networking site [online], http://in.myspace.com/ [Accessed December 31, 2010].

[5] Facebook fact sheet [online] http://www.facebook.com/press/info.php?statistics [Accessed January 2, 2011]

[6] Nielsen, "Social networking and blog sites capture more internets time and advertising," Nielsen Wire. http://blog.nielsen.com/nielsenwire/online_mobile/social-networking-and-blog-sites-capture-more-internet-time-and-advertising. [Accessed January 5, 2011].

[7] Security threat report 2010 [online], http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf[Accessed January 5, 2011]

[8] Top five social networking business threats [online], http://www.zdnetasia.com/top-5-social-networking-business-threats-62060912.htm [Accessed January 6, 2011]

[9] Wanying Luo; Qi Xie; Hengartner, U.;, "FaceCloak: An Architecture for User Privacy on Social Networking Sites," Computational Science and Engineering, 2009. CSE '09. *International Conference on* , vol.3, no., pp.26-33, 29-31 Aug. 2009.

[10] Aimeur, E.; Gambs, S.; Ai Ho; , "Towards a Privacy-Enhanced Social Networking Site," Availability, Reliability, and Security, 2010. ARES '10 International Conference on , vol., no., pp.172-179, 15-18 Feb. 2010.

[11] S. Guha, K. Tang, and P. Francis, "NOYB: Privacy in Online Social Networks," in Proc. of 1st Workshop on Online Social Networks (WOSN 2008), August 2008, pp. 49–54.

[12] Leucio Antonio Cutillo, Refik Molva, Thorsten Strufe. Safebook: a privacy preserving online social network leveraging on real-life trust. IEEE Communications Magazine, Vol 47, N°12, December 2009, pp 94-101.

[13] Chia-Lung Hsieh; , "Privacy Disclosure: Personal Information and Images on Social Networking Sites in Taiwan," Applications and the Internet, 2009. SAINT '09. Ninth Annual International Symposium on , vol., no., pp.294-295, 20-24 July 2009.

[14] Xi Chen; Shuo Shi; , "A Literature Review of Privacy Research on Social Network Sites," Multimedia Information Networking and Security, 2009. MINES '09. International Conference on , vol.1, no., pp.93-97, 18-20 Nov. 2009.

[15] Wanying Luo, Qi Xie, Urs Hengartner. "FaceCloak: An Architecture for User Privacy on Social Networking Sites" Computational Science and Engineering, 2009. CSE '09. International Conference on, Vol. 3 (31 August 2009), pp. 26-33.

[16] Ai Ho; Maiga, A.; Aimeur, E.; , "Privacy protection issues in social networking sites," Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on , vol., no., pp.271-278, 10-13 May 2009.

[17] Leudo Antonio Cutillo, Refik Molva, and Thorsten Strufe. 2009. Privacy preserving social networking through decentralization. In Proceedings of the Sixth international conference on Wireless On-Demand Network Systems and Services (WONS'09). IEEE Press, Piscataway, NJ, USA, 133-140.

[18] Mohammad Mannan, Paul C. van Oorschot(2008) on Privacy-Enhanced Sharing of Personal Content on the Web. In Proceedings of the WWW (2008).

[19] Andrew Besmer and Heather Lipford. 2009. Tagged photos: concerns, perceptions, and protections. In Proceedings of the 27th international conference extended abstracts on Human factors in computing systems (CHI '09). ACM, New York, NY, USA, 4585-4590.

[20] A. Felt and D. Evans, "Privacy Protection for Social Networking Platforms" W2SP, May 2008.

[21] W.M. Bulkley, "Online compliments can haunt you, too," Digits, Sep. 2009. http://blogs.wsj.com/digits/2009/09/18/online-compliments-can-haunt-you-too/ [Accessed September 19, 2009]

[22] ComScore, "Social networking sites account for more than 20 percent of all U.S. online display ad impressions," Sep. 2009. Available at http://www.comscore.com/Press_Events/Press_Releases/2009/9/Social_Networking_Sites_Account_for_More_than_20_Percent_of_All_U.S._Online_Display_Ad_Impression[Accessed]
[23] ComScore," Russia has World's Most Engaged Social Networking Audience,"Sep,2009.Available at http://www.comscore.com/Press_Events/Press_Releases/2009/7/Russia_has_World_s_Most_Engaged_Social_Networking_Audience.[Accessed
[24] CBCNews. Concordia bans Facebook access on campus computers 2008 [cited 28-09-2008];http://www.cbc.ca/consumer/story/2008/09/17/mtl-concordiafacebook0917.html [Accessed on Jan 25, 2011]
[25] Aimeur, E.; Gambs, S.; Ai Ho; , "UPP: User Privacy Policy for Social Networking Sites," Internet and Web Applications and Services, 2009. ICIW '09. Fourth International Conference on , vol., no., pp.267-272, 24-28 May 2009.

Chandan, New delhi, India, born in 1987 did his diploma in engineering (Electronics) from Aligarh Muslim University, Aligarh, India in 2006. Then after he did his engg degree in computer science from Guru Gobind Singh Indraprastha University, New Delhi India in 2009. Then he joined Indian Institute of Information Technology, Allahabad for MS in Cyber law & Information Security & and awarded with Master degree in 2011. Before joining IIIT Allahabad he joined Defense Terrain Research Lab, DRDO during summer Internship of Engineering Program which is a Unit of Ministry of defense Government of India. His summer Interns During Master was from K R Information Security Solutions, New Delhi, where he worked on Vulnerary Assessment & Penetration Testing, Network Security & Application Security.
His research area is related to "privacy Issue in online Social networking, Network Security, Identity & Access Management.

Rajesh H. Jayaswar, is from Mumbai and he was born in Varanasi on 11, Sept 1985.He completed his post graduation in computer science from Mumbai University, Mumbai, Maharashtra, India in 2007. After that in 2011 he completed MS in cyber law and information security from Indian institute of information technology, Allahabad, Uttar Pradesh, India. He did his summer internship from PC computer, Mumbai in the field of web application security and audit. He also wrote research paper on privacy issue of social networking sites in his final year research project. He is certified ethical hacker, certified from EC-Council. His research interest is in the field of identity and access management and cryptography.

Jayanti Arora, is born at Allahabad on 17th December, 1987. Jayanti Arora did her 10th and 12th standard from C.B.S.E Board in the year 2003 and 2005 respectively. Jayanti Arora did her B.tech in computer science discipline (2005-2009).Jayanti Arora did her masters in MS in Cyber Law and Information Security from IIIT-Allahabad(2009-2011). She did her internship at LECPL, Delhi on FTP Security and Forensics. Her paper Safe-space: Privacy issues of social networking sites got published in ICIEM, 2011, IEEE sponsored International Conference.

Bhawana Srivastava, was born in Lucknow, India in 1983. Mrs. Bhawana is Engineering graduate in Computer Science and currently she is Assistant Professor in Computer Science Department in Echelon Institute of Technology, Faridabad, India. Bhawana has made few contributions in Data-Warehousing and Data mining domain.

She four years of teaching experience serving as Assistant professor and Senior Lecturer of Computer Sceince and Information Technology in premier institutes. She has also served Hindustan Aeronautics Limited as intern in year 2004.

Rishi Raj Srivastava, was born in Allahabad, India in 1985.Rishi is M.S in Cyber Law and Information Security (2011) from Indian Institute of Information Technology, Allahabad, India and also a graduate in Computer Science and Engineering. Rishi is interested in various fields of Information Security and is working towards enhancement of internet security by developing and improving architecture and security features for various services He has a good academic record and is currently working with a leading IT firm as ASE where his prime responsibility is Vulnerability Assessment ,Pen-testing and Consulting clients with Information Security Risks. He has worked in Tata Consultancy Services, Gurgaon, India as intern in domain of application security.Mr. Rishi has received meritorious student award from Governor of U.P Late Dr. Vishnu Kant Shashtri in 2001 and numerous other awards in various curricular and extracurricular activities.