Computer and Information Science; Vol. 6, No. 1; 2013
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Paradigm Shift in the Security-n-Privacy Implementation of Semi-Distributed Online Social Networking

Yasir Ahmad[1] & Abdullah Aljumah[2]

[1] Department of Computer Science, Salman Bin Abdulaziz University, Saudi Arabia

[2] Department of Computer Engineering, Salman Bin Abdulaziz University, Saudi Arabia

Correspondence: Yasir Ahmad, Department of Computer Science, Salman Bin Abdulaziz University, Saudi Arabia. E-mail: y.ahmad@sau.edu.sa

Received: October 14, 2012 Accepted: December 18, 2012 Online Published: January 28, 2013

doi:10.5539/cis.v6n1p140 URL: http://dx.doi.org/10.5539/cis.v6n1p140

Abstract

Social Networking Applications has gained tremendous response from all the sections of people across the entire world from last few years. Social networking has crossed all the boundaries and glued whole world population together. Users of OSN (Online Social Networking) sites can re-connect with school friends, find some activity or even life partners, and make new friends. OSN has also revolutionized the business community. Now the companies leverage OSN's credibility and build their reputation, get invaluable information about the customers. The companies are also using OSN for the advertising and the recruitment processes. However, posting of user information on OSN poses greater threats/risks as identity theft, online stalking, and information leakage. The volume and accessibility of personal information available on social networking sites have attracted malicious people who seek to exploit this information. This imposes greater threat to the users' privacy and security. In this article many security and privacy challenges currently faced by OSN applications are mentioned. The distributed OSN architecture with an external control module is proposed and a prototype is also presented which overcomes many of the privacy, security, accessibility and identity challenges in different perspectives faced by current OSN applications.

Keywords: access control, control module, data privacy, distributed OSN, validation key

1. Introduction

Social networking is a new form of interacting on-line where participants in a virtual network can share information and communicate with one another (Murchu et al., 2004). Social networking and community-based online services offer great fun and many benefits, both to individual users and to organizations. Users can re-establish contact with old school friends, find activity or even life partners, create art, and make new friends. Companies can leverage them to build their brand, get invaluable information about what their customers really think, and fix problems as they arise, among many other value-adding activities. However, social networking sites can also be a source of personal information leaks. They can also become a malware attack vector, when not used cautiously (Trendmicro, 2009). All the current social networking sites offer a lot of interesting functionality but also bring potential problems related to privacy, information accountability and ownership of information (Buchegger et al., 2009). The increasing risk of misuse of personal data processed by online social networking applications is evident from computer science research (Nissenbaum, 2006; Helen et al., 2004; Cranor & Lorrie, 2003).

The centralized OSN model, widely adopted by prevailing social networks, makes an explicit trade-off that maintain viable monetary incentives for the provider at cost of sacrificing user control on their own data. In this "walled garden" OSN architecture, all personal information, social data, and relationships are exposed to a single provider, who can generate revenue through content-driven ads placement, or in some cases, selling user datasets. In contrast, distributed OSN architectures take the opposite extreme; total privacy (www.w3.org, 2009). Replacing centralized OSN providers with peer-to-peer (P2P) services (Buchegger et al., 2009; Antonia & Grand, 2009), where no central authority can claim the right to exploit the data, is a proposal that is achieving widespread success among the scientific community.

We also propose a distributed architecture of OSN application in which the OSN service provider only needs to store the core application part i.e., basic users' information and social graphs on their servers. The user data like photos, videos, messages etc. are stored in the user systems to increase the availability, and decrease the latency time. And at the same time from the service providers' perspective optimal resources and costs are required to implement the application at their data centers. There is also an external control module installed with the core application which controls the identity, and accessibility to the users' data and dynamically generates the privacy settings for the friends and FOAF.

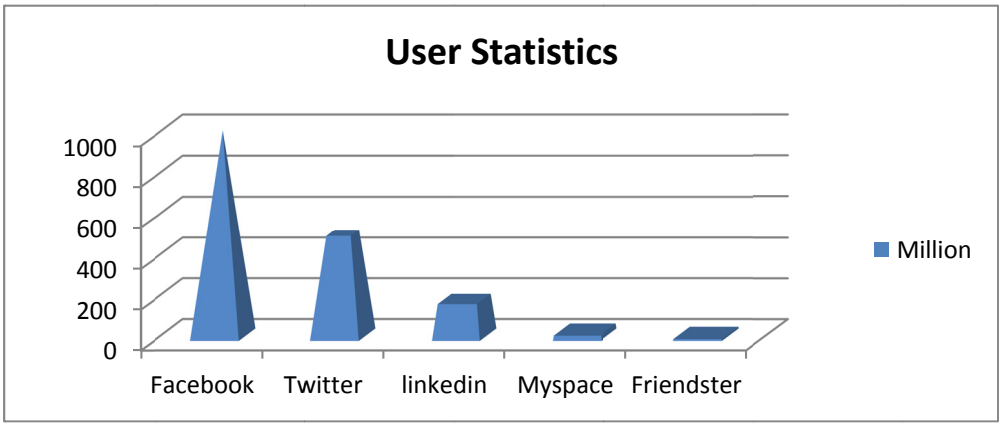

Figure 1. User statistics graph

Rest of the paper is organized as; section 2 describes the user statistics of various OSN's, section 3 describes the strengths, section 4 challenges, section 5 related work, section 6 proposed architecture, and section 7 conclusion and future work.

2. User Statistics

Social networking sites like Facebook, Twitter, Youtube, MySpace and others are now the most visited social networking sites (searchenginejournal.com) and they have the huge user base across the world as evident from the Figure 1. Facebook claims that they have 800 million active users and 50% of the active users log on to Facebook in any given day. Average user has 130 friends. More than 7 million apps and websites are integrated with Facebook (Facebook). The survey, fielded by Rebtel CEO Andreas Bernstrom; conducted on 2361 U.S. adults over the age of 18 reveals that woman significantly lead men when it comes to social networking (mashable.com, 2011).

68% of women and 54% of men use social media to stay in touch with their friends.

60% of women and 42% of men use social media to stay in touch with their family.

34% of women and 22% of men use social media to stay in touch with their co-workers.

Nine of the 10 most popular social networks were dominated by women. Only LinkedIn had a percentage of men visiting the site that exceeds the percentage of men who are active Internet users (Social Media Report, 2011).

The total (not exhausted) numbers of users and the launched year of various OSN websites are collected through the online survey which is clearly depicted in the Table 1. The collected user statistics clearly shows; at which pace the users of various OSN applications are increasing in numbers from last few years. And these numbers are increasing exponentially. The figures showed in the Table 1 makes a serious challenge to current OSN sites to protect the users' data, privacy, and identity.

Table 1. Number of OSN users

Online Social Networking Site	Launched (Year)	Total Users (2012) in millions
Facebook	2004	1000
Twitter	2006	500
LinkedIn	2003	175
MySpace	2003	25
Friendester	2002	8.2

In section 4 we have mentioned some of the security and privacy challenges currently faced by OSN sites. And in section 6; the proposed architecture tried to overcome these challenges. However, it was not possible to overcome all the challenges currently faced by online social networking sites.

3. OSN Strengths

A few of OSN strengths are mentioned below:

1) People could interact with new people and their already known acquaintances, where in person contact is not possible.
2) Greater number of people could be reached by posting information on the wall.
3) Lot of other useful services is available through the third party applications accessible within the sites.
4) Users reach ability is inevitable with friends and relatives across the world.
5) Business communities' utilizes it to build their brands and for advertising purposes. They could deliver improved customer service and respond effectively to feedback.
6) "Poking" has become the new handshake.
7) It's a great way to get you known in the network in your field or industry.
8) Social networking could be used to get feedback on ideas immediately.
9) Social networking could be a great way for students to get in touch with other students in the same school.
10) Social Networking sites offer students the opportunity to create a positive self-image. The profiles give them a chance to create the image of themselves that they want people to see by putting their best qualities.

4. Security and Privacy Challenges

Apart from the strengths discussed above, current OSN applications have a certain number of security and privacy concerns some of which are listed below:

1) A user has no absolute control over the information posted by her, whoever has access to it.
2) The privacy settings in the OSN sites are static in nature (Liu et al., 2011).
3) Any user could post information about you, either favorable to you or vice-versa.
4) Cross-Site Scripting (XSS), identity theft, phishing, and social engineering attacks are common on OSN sites (Hashimoto et al., 2010).
5) The things (Note 1)we post could live there forever.
6) Personal life and business matters are more exposed.
7) Sometimes posting personal information about your vacation, etc could put your life in danger.
8) The application provider could sell the user data to third party application providers, business communities etc for the financial gain (Gao et al., 2011).
9) Attackers can spread worms and establish botnets more easily because of the rich and frequent interactions in the OSN. Malware can propagate over social networks via profile, interaction, and third-party applications (Luo et al., 2009).

10) The personal information is very useful to attackers. Privacy such as password, bank account and social security number are the very thing attackers are looking for. Once attackers gain these information they can commit further crimes, even identity theft (Cutillo et al., 2009).
11) In social networks attacker can disguise himself as a legitimate user and uses social engineering to entice other users to click the designed URL. Users in social networks are willing to accept the invitation of strangers and communicate with them. This will lead to a phishing attack (Cutillo et al., 2009).
12) The enormous amount of digital information about the users (i.e, profiles, photos, videos, messages ect.) is located on a single centralized server which poses a greater threat to users privacy and security.

5. Related Work

Cutillo et al. (2009) proposed decentralized OSN based on a P2P architecture whereby basic security and privacy problems as well as the lack of a priori trust and incentives are addressed by leveraging on real-life trust between users, such that services like data storage or profile data routing are performed by peers who trust one another in the social network. It consists of three-tier architecture with a direct mapping of layers to the OSN levels. The user-centered social network layer implementing the SN level of the OSN. The P2P substrate implementing the AS Services. The Internet, representing the CT level each party is thus represented by a node that is viewed as a host node in the internet a peer node in the P2P overlay, and a member in the SN layer. In addition to these nodes, it also features a trusted identification service (TIS), providing each node unambiguous identifiers: the node identifier for the SN level and a pseudonym.

Monica et al. (2009) proposed distributed platform that retains the core functionalities of a centralized service with the additional advantage of returning ownership of the data to the user. The existence of a distributed solution offers consumer choice and puts pressure on centralized services to treat the data with the care and discretion they desire. A distributed, technically more efficient, platform may even supplant centralized services if privacy can be monetized to generate new classes of viral applications and more effective targeted marketing.

Geambasu et al. (2007) describes a P2P middleware solution that enables users to share personal data based on pre-created views that are based on a SQL-like query language. Access is managed using capabilities, which are cumbersome for a client to carry, can be accidentally shared, broadcasted and are harder to revoke.

The PeerSon system (2009) is one of the first P2P design for a OSN. The goal of user information privacy is achieved through symmetric encryption of content stored in a DHT. The P2P network serves mainly as a lookup service: once the two endpoints' contacts have been retrieved from the DHT, direct connections are established. When a friend is offline, update notifications are managed asynchronously through the DHT using a pull approach. Full decentralization and encryption prevent, respectively, the ''Big Brother'' effect and network crawling activities aimed to data collection. However, advanced access control features like highly dynamic group membership are not taken into account.

In Graffi et al. (2009) authors propose a DHT-based storage with access control capabilities for social shared resources. Encrypted items are published together with several copies of the secret key; each copy is encrypted with the key of a user who has access permission for that resource. A drawback of this solution is that when the access control list of a specific content must be changed, a new updated item has to be built and stored again. User registration phase and secure P2P communications are inspected as well.

Narendula et al. (2010) proposed an initial design of such a system, referred to as porkut, where users organize a social network over a P2P overlay with privacy-preserving data access. They briefly outline the system architecture and mainly focus on the distributed storage layer. Specifically, they propose a decentralized mechanism for users to manage their own online social network on top of resources collectively contributed by themselves. Such a design is motivated with several goals in mind: a) It eliminates the requirement for a single big brother who can exploit the users' profile data for his own interest without users' consent. b) It preserves the privacy of individual's social profile content, as they have complete control on who can access which parts of the content. c) It exploits the trust relationships among users in the social network to improve the content availability and the storage performance.

Krishnamurthy and Wills (2009) showed that most users on OSNs are vulnerable to having their OSN identity information linked with tracking cookies. Unless an OSN user is aware of this leakage and has taken preventive measures, it is currently trivial to access the user's OSN page using the ID information. The two immediate consequences of such leakage: First, since tracking cookies have been gathered for several years from non-OSN sites as well, it is now possible for third-party aggregators to associate identity with those past accesses. Second,

since users on OSNs will continue to visit OSN and non-OSN sites, such actions in the future are also liable to be linked with their OSN identity.

6. The Proposed Architecture

The proposed architecture relies on the conventional distributed approach however some modifications are possible according to the needs of a particular OSN provider; the DOSN application provider needs to store only the core application part, basic user info, and the social graph which facilitates the user communication. Social graphs as a whole are stored at service provider's end, and the replicas of small network graphs are stored at each users end consisting her network of friends. The users' wall posts, videos, photos, inbox messages Access Control Lists are stored in the user systems. However, it is not possible that each and every user system could be available (Note 2) round the clock, so the data stored in the user system is replicated among different users in her network of friends so as to maintain the availability of the data all the time. Although the architecture is distributed; the service provider could easily utilize the core application part for advertising and third party services like games etc for their monetary gain without affecting the user's privacy. A limited scenario between a single user system and application server (data center) is shown in Figure 2.

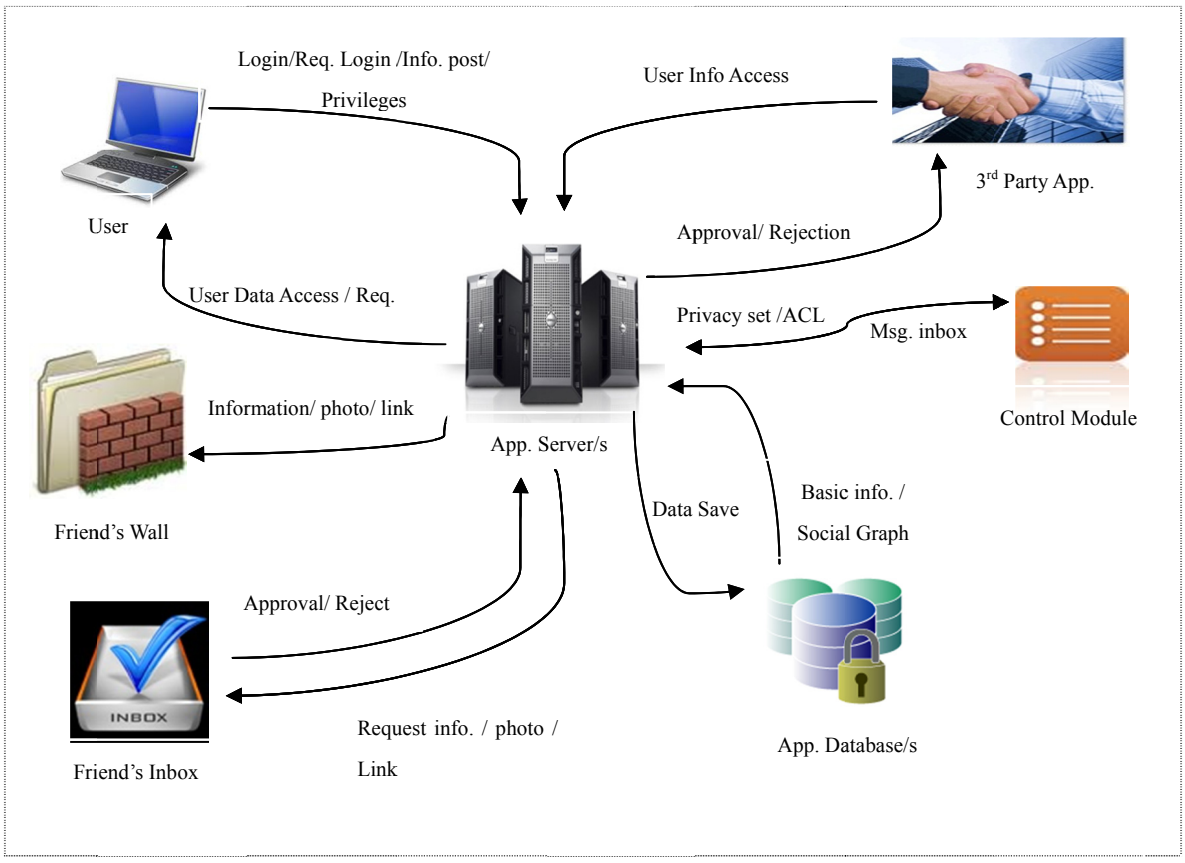

Figure 2. A single user scenario

Accessibility: An Access Control List (ACL) is a table that tells which access rights each user has to a particular user object (Note 3). Each object has a security attribute that identifies its access control list. The list has an entry for the object with access privileges. The most common privileges include the ability to read, to write, to modify, to delete and to view the pictures and videos. An access control list (ACL) is associated with each user object. Each ACL has one or more access control entries (ACEs) consisting of the name of an owner and other users. This ACL facility is devised into the architecture to control the access to the user data. The Access Control List (ACL) is stored along with the user data in the user systems. The user data is replicated across the network of her friends with the ACL. Only the owner of the data to which the data belongs could give privileges to other users to access her data as shown in the Table 2.

Table 2. User privileges

	Read	Write	Modify	Delete	Post
User (Owner)	✓	✓	✓	✓	✓
Friend	✓	✓			✓
FOAF	✓				
Public	✓				

Control Module: It is an algorithm shown below designed for the specific purpose integrated with the core application which works as follows; firstly, when a new user registers in the DOSN application, the control module requires filling a validation key (Note 4) from the user along with the other fields; it may be her phone number, address, or anything which uniquely identifies that user. Then the user data; name, password, location, date of birth, phone number etc is stored in the same user system. An access control (Note 5) mechanism is devised to control the access to the user data.

Algorithm:

```
Start
If un, pw is true
      goto c;
else
      goto g;
Add f;
pcy = true;
Read m;
inbx = m;
       If retVal(inbx) = = true
              p = true;
              goto j;
         Else
             goto e;
r = true;
ak = true;
goto b;
Stop
```

This access control mechanism is applied to all the replicas and ensures that the user data is safe. None of the following; adversary, third party application providers and the business communities could access the user information directly (Note 6) or even with the service providers consent. If a third party application wants to access the user information, a formal request has to be sent via the service provider's interface to the user's inbox for the verification and for approval. The approval/rejection is at the sole discretion of the user.

Secondly, when a user posts any message on the friend's wall before the message is displayed the control module sends the same message to the targets inbox (Note 7). When the target approves the message, then only the same is displayed on her wall. This mechanism prevents every user to post any type of information on their friend's walls without the consent of the target user. Thirdly, when the user adds a new friend in her list, the privacy settings are dynamically generated by the control module for this friend. So, every time a user adds new friend to her list, she has to set the privacy settings for that contact. These privacy settings are editable. Users could

change the existing privacy settings as per the requirement later. Lastly, the privacy settings for the friend-of-a-friend remain same as are with the newly added friend.

Some notations used in the following algorithm are 'un' is the username, 'pw' is user the password, 'r' is registration variable, 'p' is used for the publish option,'m' is the message, 'f' is the friend variable, and 'ak' is used as access key, 'pcy' is used for privacy setting variable, 'inbx' is the friend inbox variable.

6.1 Working Steps

The algorithm shown is summarized into the following points:

Case I: If the user is registered:

- The user adds a new friend in her list with the new dynamic privacy settings for that user.
- The user requests to post a message on her friend's wall or a photo view.
- The control module forwards this request to the friend's inbox for the verification with the approve / delete option.

If the friend approves the request, it is published on the friend's wall.

Case II: If the user is not registered:

- The user has to register herself with the application by providing the validation key along with all details.
- The control module generates an access control list and stores it with user data.
- Now the user is ready to login.

6.2 Advantages

1) Distributed architecture of OSN application could be utilized for more availability, security, privacy of user data, which is considered to be the most important requirement for current OSNs.
2) The de-centralization of the OSN increases the availability of the network for the users and prevents the D-O-S attacks (Kryczka et al., 2009).
3) The privacy settings for the newly added contacts are dynamic with the inclusion of control module with the application.
4) As far as security is concerned the user data (photos, videos, messages etc.) is stored in the user systems with an access control mechanism.
5) Privacy of users' data is maintained by utilizing the relationships among the users and the verification/approval of data to be displayed by sending the notification to the users' inbox.
6) The distributed architecture of OSN is robust via the detection and cleaning of malicious and infected nodes in the network (Duma et al., 2006; Fung et al., 2008).
7) A user could write on the wall; view the photographs of her friend only if she has the required privileges in the ACL, after getting the required permission from her friend or acquaintance.
8) At the time of registration a user has to fill a key which uniquely identifies that user, so there is no possibility of anonymous users.
9) Low implementation costs for service providers as the provider only needs to store basic user info, social graphs and core application part the rest of the user data is stored in the user systems.
10) With the help of unique validation key users' identity in the system is protected from any identity theft.
11) With the help of same validation key the program bots could not register and appear as legitimate user in the system.

6.3 Drawbacks

1) The user data for the availability purpose is replicated among many user systems that make the data redundant.
2) All the data in the system is distributed in nature so the data Synchronization must be maintained all the time.
3) Advanced routing algorithms (Note 8) need to be implemented at the routers.
4) The requirement of validation key for the registration purpose by the application; some users are reluctant to disclose any kind of personal information.

5) Maximum uptime of user systems to maintain the data availability.
6) The user could post any type of information on her own wall about herself, friends, friend-of-a-friend or anybody else.

7. Conclusion

By implementing the proposed architecture, OSN's will be more secure, and reliable rather than having the threat of losing the privacy of users information, the user data and identity will be more secured in this architecture. However, there are some disadvantages related to this system which are discussed in section 6.2; while designing the architecture users concerns were considered to be more important. Social networking is meant to bring people with similar interests together. These sites allow people to communicate with each other and meet people with similar ideas. OSN is a great tool for business purposes if used correctly, the business communities are now turning to various OSN's to increase their product advertisement and awareness. Information spreads faster through OSN than a real life network. And this information sometimes harm the users; when it travels through spheres, and ends up with the people to whom it was not intended for. This poses a serious threat over the user's privacy, and security. The Proposed Distributed Architecture addressed some common privacy, security, and accessibility challenges faced by the OSN's today. In our future work we will consider some type of control over the users own wall postings and more concrete mechanism to prevent program bots registering with the applications and will also try to overcome more privacy, security and accessibility challenges with the current OSN's.

References

Antonia, P., & Grand, B. L. (2009). Self-organised virtual communities; bridging the gap between web-based ommunities and P2P systems. *International Journal of Web Based Communities, 5*(2), 179-194. http://dx.doi.org/10.1504/IJWBC.2009.023964

Buchegger, S., Schiöberg, D., Vu L. H., & Datta, A. (2009). PeerSoN: P2P Social Networking - Early Experiences and Insights. In *Proceedings of the Second ACM EuroSys Workshop on Social Network Systems* (pp. 46-52). New York, NY: ACM.

Ching-man, A. Y., Ilaria, L., Kanghao, L., Oshani, S., & Tim, B. L. (2008). *The Future of Online Social Networking*. Retrieved from http://www.w3.org/2008/09/msnws/papers/decentralization.pdf

Cranor, F. L. (2003). 'I Didn't Buy it for Myself' – Privacy and EcommercePersonalization. In *Proceedings of the 2003 ACM workshop on Privacy in the electronic society* (pp. 111-117). Washington DC, USA. http://dx.doi.org/10.1145/1005140.1005158

Cutillo, A., Molva, R., & Strufe, T. (2009). Privacy preserving social networking through decentralization. In *Proc. of the 6th International Conference on Wireless On-demand Network Systems and Services*. http://dx.doi.org/10.1109/WONS.2009.4801860

Cutillo, L. A., Molva, R., & Strufe, T. (2009). Safebook: A privacy-preserving online social network leveraging on real-life trust. *Communications Magazine, IEEE, 47*(12), 94-101. http://dx.doi.org/10.1109/DEXA.2006.21

Duma, C., Karresand, M., Shahmehri, N., & Caronni, G. (2006). A Trust-Aware, P2P-Based Overlay for Intrusion Detection. In *17th International Conference on Database and Expert Systems Applications (DEXA'06)* (pp. 692-697). http://dx.doi.org/10.1109/DEXA.2006.21

Fung, C. J., Baysal, O., Zhang, J., Aib, I., & Boutaba, R. (2008). Trust Management for Host-Based Collaborative Intrusion Detection. In *Proceeding DSOM '08 Proceedings of the 19th IFIP/IEEE international workshop on Distributed Systems: Operations and Management: Managing Large-Scale Service Deployment* (pp. 109-122).

Gao, H., Hu, J., Huang, T., Wang, J., & Chen, Y. (2011). Security Issues in Online Social Networks. *Internet Computing, IEEE, 15*(4), 56-63. http://dx.doi.org/10.1109/MIC.2011.50

Geambasu, R., Balazinska, M., Gribble, S. D., & Levy, H. M. (2007). Homeviews: Peer-to-peer middleware for personal data sharing applications. In *Proceedings of the 2007 ACM SIGMOD International Conference on Management of Data* (pp. 235-246). http://dx.doi.org/10.1145/1247480.1247508

Graffi, K., Mukherjee, P., Menges, B., Hartung, D., Kovacevic, A., & Steinmetz, R. (2009). Practical security in p2p-based social networks. In *LCN'09: 34th IEEE Conference on Local Computer Networks*. http://dx.doi.org/10.1109/LCN.2009.5355085

Hashimoto, G. T., Rosa, P. F., Filho, E. L., & Machado, J. T. (2010). A Security Framework to Protect against Social Networks Services Threats. In *2010 Fifth International Conference on Systems and Networks Communications*. Washington, D.C.: IEEE Computer Society. http://dx.doi.org/10.1109/ICSNC.2010.36

Huber, M., Mulazzani, M., & Weippl, E. (2010). Social Networking Sites Security: Quo Vadis. In *2010 IEEE Second International Conference on Social Computing (SocialCom)* (pp. 1117-1122). http://dx.doi.org/10.1109/SocialCom.2010.166

Jinyuan, S., Xiaoyan, Z., & Yuguang, F. (2010). Privacy and security for online social networks: challenges and opportunities. *IEEE Network, 24*(4), 13-18. http://dx.doi.org/10.1109/MNET.2010.5510913

Krishnamurthy, B., & Wills, C. E. (2009). On the leakage of personally identifiable information via online social networks. In *Proceedings of the 2nd ACM workshop on Online social networks (WOSN '09)* (pp. 7-12). New York, NY: ACM.

Kryczka, M., Cuevas, R., Guerrero, C., Eiko, Y., & Azcorra, A. (2010). A first step towards user assisted online social networks. In *Proceeding SNS '10 Proceedings of the 3rd Workshop on Social Network Systems*. New York, NY: ACM.

Lam, M. S. (2009). *An Exploration of Distributed Social Networking*. Retrieved from http://suif.stanford.edu/~lam/pepm.pdf

Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). Analyzing Facebook privacy settings: User expectations vs. reality. In *Proceedings of the 11th Usenix/ACM Internet Measurement Conference* (IMC). Berlin, Germany.

Lua, E. K., Crowcroft, J., Pias, M., Sharma, R., & Lim, S. (2005). A survey and comparison of peer-to-peer overlay network schemes. *IEEE Communications Surveys and Tutorials, 7*(2), 72-93. http://dx.doi.org/10.1109/COMST.2005.1610546

Luo, W., Liu, J., Liu, J., & Chengyu, F. (2009). An Analysis of Security in Social Networks. In *Dependable, Autonomic and Secure Computing, 2009. DASC '09. Eighth IEEE International Conference* (pp. 648-651). http://dx.doi.org/10.1109/DASC.2009.100

Madden, M., & Fox, S. (2006). *Riding the Waves of Web 2.0*. Retrieved from http://www.pewinternet.org/Reports/2006/Riding-the-Waves-of-Web-20.aspx

Murchu, I. O., Breslin, J. G., & Decker, S. (2004). *Online Socialand Business Networking Communities*. Digital Enterprise Research Institute, NUI Galway, Ireland.

Nielsen. (2011). *Social Media Report: Q3, 2011*. Retrieved from http://blog.nielsen.com/nielsenwire/social/

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review, 79*, 101-115.

Narendula, R., Papaioannou, T. G., & Aberer, K. (2010). Privacy-Aware and Highly-Available OSN Profiles. In *Proceedings of the 2010 19th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE '10)* (pp. 211-216). IEEE Computer Society, Washington, DC, USA.

Notes

Note 1. Whatever type of information user posts on the wall.

Note 2. It is not possible to keep every user system online round the clock.

Note 3. User object is a complete set of a user's data like photos, messages, profile info, videos etc.

Note 4. This is how we protect identity theft in our DOSN Application and also prevents the program bots to register with the system.

Note 5. An access control list (ACL) is created for each user and is stored along with the user information. Only the user to which the data belongs has privilege to access or give access to her data.

Note 6. As the data is distributed in nature and is not accessible.

Note 7. The registered email of the user which she entered at the time of registration with the OSN application.

Note 8. To facilitate the smooth flow of network traffic and optimal network paths.