USER PRIVACY PROTECTION IN ONLINE SOCIAL NETWORKS: SECURE FILE SHARING ON FACEBOOK

Muhammad Umar Chaudhry, Yasir Saleem, Muhammad Munwar Iqbal
[1,2,3] Department of Computer Science and Engineering, University of Engineering and Technology, Lahore, Pakistan.
[3]Department of Computer Science, University of Engineering and Technology, Taxila, Pakistan
umar_age85@yahoo.com, ysaleem@gmail.com, munwariq@gmail.com

ABSTRACT- *Online Social Networks (OSNs) are more prevalent these days, over 900 million users share their personal information on them. But OSN user's privacy is under risk as their shared content is visible to the OSN service providers. This is due to the fact that OSNs have centralized servers in which user's information is stored and they have complete control of user's information stored on their servers. User's personal information, pictures or blogs can be taken by the service providers easily as they are hidden from other users but not from OSN service providers. OSNs use this information for different business purposes, e.g. can sale data to marketing companies. This action is seriously against their claim of keeping privacy of their users intact. Many other security breaches are also present, but the shared content visibility is the most critical issue. A lot of research work is being done to ensure the privacy of OSN users, but not completely eliminated this problem yet. In this research a cryptographic framework is proposed to implement OSN user's privacy by eliminating the intrusion of the unauthorized access. Based on the proposed framework, an application is built that runs on the OSN website at the user's end. This application encrypts the user's content shared on OSN and only legitimate users will be able to decrypt that shared content, thereby achieving privacy goal.*

Keywords: Online Social networks (OSNs), Facebook, Secure File Sharing System, Cryptography

INTRODUCTION

Online Social networks (OSNs) are the huge web portal for the millions of users to access the Internet. These networks entrusted the users to share information with their friends. On a social network, e.g. Facebook; a user can share personal information, phone numbers, occupation, religious view, photograph, etc. Figure 1 shows the percentage usage of different OSNs.

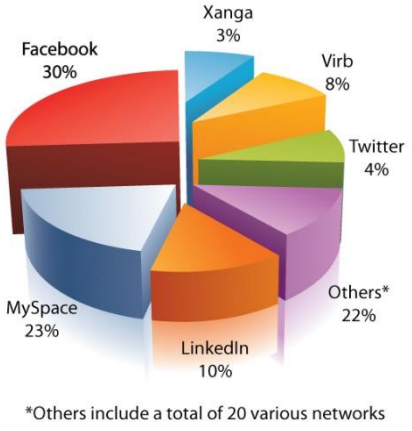

Figure 1: Social Networks Usage

A figure of debate is to make a methodology that enhances the user privacy on the centralized network. As the shared data content of the users is stored on centralized servers of the service providers and they have complete control over the data stored. This creates the problem of privacy and security for the users as their private data can be misused and breached. Also there are some limitations in privacy settings of existing OSNs as the user cannot completely restrict his private data to be shown only to his specified relations. Thus, a methodology is proposed on the basis of encryption. A key distribution mechanism is employed to secretly distribute keys to the authorized users. Based on encryption scheme an application is developed to encrypt the data before sharing while running on the client side of OSN website. This scheme will enhance user's privacy while using OSN.

In OSN like Facebook, privacy controls are also available to enable the user to customize his privacy [1]. But these controls are not able to restrict the application developers or the service provider to get user's private information, as all the content is stored on OSN provider's huge servers. On Facebook, lets the users to endow provider the right to sell the information to others after using some Facebook applications. The "Statement of Rights and Responsibilities" [9] of the Facebook states that "user must not provide any false information and keep the contact up to date", it also makes another statement "Facebook is a non-exclusive, transferable, royalty-free worldwide license to use any intellectual property content that post on or in connection with Facebook". Regardless of these statements the tools provided by the Facebook don't ensure the user privacy protection. Many tools and techniques have been developed to resolve the security breaches faced by the Facebook.

Cryptography is the main tool for maintaining privacy. The major task of the cryptography in OSN perspective is to restrict information in the appropriate range. This range is defined in terms of relationships of a user. A user's family, neighbour, co-worker, boss and any other relations of that kind are taken as relationship in OSNs. We simply define these relationships as a "Friend". Key management is a very efficient way of ensuring access control also for managing groups. The user will encrypt his content prior to sharing on OSN website [2]. Key management scheme will provide the secret keys to all the legitimate users. By using the secret keys, users can decrypt and access the content.

Thus, a methodology is proposed on the basis of encryption. A key distribution mechanism is employed to secretly distribute keys to the authorized users. Based on encryption scheme an application is developed to encrypt the data before sharing while running on the client side of OSN website. This scheme will enhance user's privacy while using OSN. Users possessing shared secret key will be able to see the shared content on OSN website. The objective of this research work is to plan an application that has the following properties:

- It will enhance the user privacy protection by employing encryption.
- It will reduce the privacy breaches done by OSN service providers.
- It will reduce the cost overhead of building new decentralized OSNs to ensure privacy. Privacy can be achieved by incorporating encryption schemes in existing centralized OSN architectures as suggested in this research.

Online Social Networks (OSNs) have turned into an imperative web administration where individuals can distribute and offer assets (individual tastes, sites, or perspectives) through diverse sorts of connections [10]. Various interpersonal organization destinations have as of late rose and they are turning into a famous and valuable approach in individuals' everyday life. The accessibility of data brings comfort to current life while altogether raising issues identified with individual protection. For example, individual private information may be utilized for advancing unnecessary items, and assets may be mishandled by some unapproved clients, and so on. Accept that a reasonable and powerful key administration access control plan ought to give the accompanying properties: 1) Autonomy, once a client joins in a private OSN, he picks his open key and private key without anyone else's input and the OSN supervisor can't acquire his private key; 2) Independence, a group is built by a situated of trusted clients and there is no outsider included; 3) Collaboration, the portion parts can team up to develop and keep up a private OSN to lessen the support many-sided quality; 4) Anonymous Authentication, OSN can confirm the legitimacy of the client's right to gain entrance consent for a private OSN without a client's character; and 5) Revocation, a group could disavow the authorization of approved clients for all time or briefly.

LITERATURE REVIEW

To build a private OSN setting, a few plans have been proposed lately. In spite of the fact that these plans received diverse cryptographic strategies, for example, conventional symmetric/uneven encryption [15,16,18,21] and in addition characteristic based encryption (ABE) [12, 20, 21] they have a same working model: to make another gathering from a rundown of known companions. Alice (the maker) scrambles a recently produced gathering key with general society key of every part of the new gathering (acquired from PKC/PKI). She then circulates this key to the parts of that gathering and uses the way to encode messages for the gathering. The data imparting can be acknowledged by trading the key inside the gatherings. In this model, the gathering key may be symmetric, in which case just gathering parts can scramble for the gathering, or hilter kilter, which permits non-parts to encode also.

Despite the fact that it looks as if this model has a straightforward structure, it actually requires not just the foundation of a PKC/PKI framework, additionally obliges a repetitive assignment of key administration for the maker. Also, the clients' open keys focused around PKC/PKI are utilized to circulate the gathering enter in this model.

Many approaches have encompassed the problem of the privacy protection in the social networks. Access control strategies are applied for privacy enhancement. Under rule-based access control a user is allowed to specify access rules for their contents [20]. Set of conditions for resource access and resource identifiers combined to make the access rule. When a requester satisfies at least one access rule by means of relation certificates he is authorized to access a resource. These rules are for the access control on the client side. Privacy of the relationship is also addressed in the recent research. A model is described to know the trusted relationship of the user to check the level of the disclosure of the user thoughts [13]. This model is analogy of the access control as the relationship certificates taken as resource are encrypted using cryptographic algorithms. Distribution rules are specified; when these rules are satisfied, the certificate of access is allowed. Certificates are encrypted and signed by using the public key for private relationships [16]. But using this scheme the intermediate users get the vision of the relationship strength. It becomes difficult for new access for that purpose the multiple users are involved in a protocol. Key management techniques are used to implement access control.

A hierarchy key management scheme was described that was tailored on hash function and CCA-secure encryption in term of relationship hierarchy of the social network. If the access graphs have the node to the node path, then key can be driven to access the data [23]. A novel scheme is also introduced to the hierarchy key management scheme [19]. Distance-based access policies are specified and access control is managed through the key management. But this scheme is decentralized. A new cryptosystem is introduced which was based on fine-grained access control scheme through attribute-based encryption [21]. Online social network architecture, Persona, hides user data using ABE. Public key cryptography authentication is used to enhance the privacy of the user data [12]. A new application fly-By-Night using traditional cryptography, in which encryption is achieved through public key on the client side and decryption of the cipher-text is done with private key [25].

The author of [5] condenses the positive values that have been connected with security in the current writing: Autonomy, counterculture, innovativeness, majority rules

system, erraticism, nobility, opportunity, flexibility of thought, fellowship, human connections, creative energy, autonomy, singularity, closeness, mental prosperity, notoriety, change toward oneself. The accompanying qualities can be added to this rundown [24]: enthusiastic discharge, singular honesty, love, identity, pluralism, determination toward oneself, admiration, resistance, evaluation toward oneself, trust.

There has been a generous measure of work tending to the issue of security insurance in interpersonal organizations. One territory of exploration is to ensure client's protection by authorizing access control. Case in point, Carminati et al. [20] proposed a standard based access control model which permitted clients to point out access principles for their substance. A right to gain entrance tenet comprises of the asset identifier and a set of conditions which must be fulfilled to be permitted to get to the asset. A requestor is approved to get to an asset just in the event that he gives the asset holder a confirmation that she fulfills no less than one of the relating access guidelines, by method for relationship declarations.

This plan implements access control at customer side. Furthermore, they proposed an instrument to authorize access control for electronic informal organizations [22]. Other than assurance of assets, some late works address the security of connections in interpersonal organizations, since accessibility of data on connections (trust level, relationship sort) offers climb to security concerns: knowing who is trusted by a client and to what degree being trusted reveal a great deal about client's musings and sentiments. Case in point, Carminati et al. [13] portrayed a right to gain entrance control show on relationship insurance. In this model, the relationship endorsements are encoded utilizing symmetric cryptographic calculation and are dealt with as an asset: a declaration is allowed stand out fulfills a dissemination standard, which is practically equivalent to the right to gain entrance tenet. Ferrer et al. [16] presented an open key convention for private connections, where authentications were encoded unevenly and marked. In any case this plan has downsides: relationship qualities are uncovered to moderate clients and it obliges numerous clients to take part in a convention for every new get to.

PROPOSED SOLUTION & IMPLEMENTATION

This research proposed an encryption scheme that simplified and more useful. Based on this encryption scheme an application is built that runs on client side and enable the users to encrypt their content before sharing. User's possessing shared secret key will be able to see the shared content on OSN website.

Our private OSN model could be implicit existing informal community stages, for example, Facebook, Orkut, and so on which typically permit designers to make "applications" to develop the sorts of data that can be put away, controlled, and imparted utilizing interpersonal organization interfaces. Fig. 2 delineates an application data flow for our structural engineering. In this model, an OSN Platform API goes about as a middleware for all collaborations between application suppliers and end clients. End clients, including bit parts, (full) approved parts, and unapproved clients, launch contact with an application supplier through a URL on OSN stages. The stages translate information alongside these appeals and pass their deciphered information by means of the Internet to the application servers, whose locations are enrolled with stages by the application engineers. The application server then performs asked for activities focused around the stage deciphered client info, maybe including database operations. The application server then conveys to the stage a yield page comprising of HTML and stage particular markup, including scripts. The stage then deciphers this yield page, supplanting the stage particular markup with standard HTML and JavaScript, and conveys the translated yield page to end clients. A cryptographic module focused around ActiveX is utilized to execute the decoding of yield pages in the customer's program.

In this structural engineering, the asset distributer implements access control through encryption and key administration on our GCC plan. In light of the above application data flow: in an interpersonal organization every client can pick a most loved mark and produce a private key without anyone else, and after that enlist her name into an OSN stage by User Register calculation;

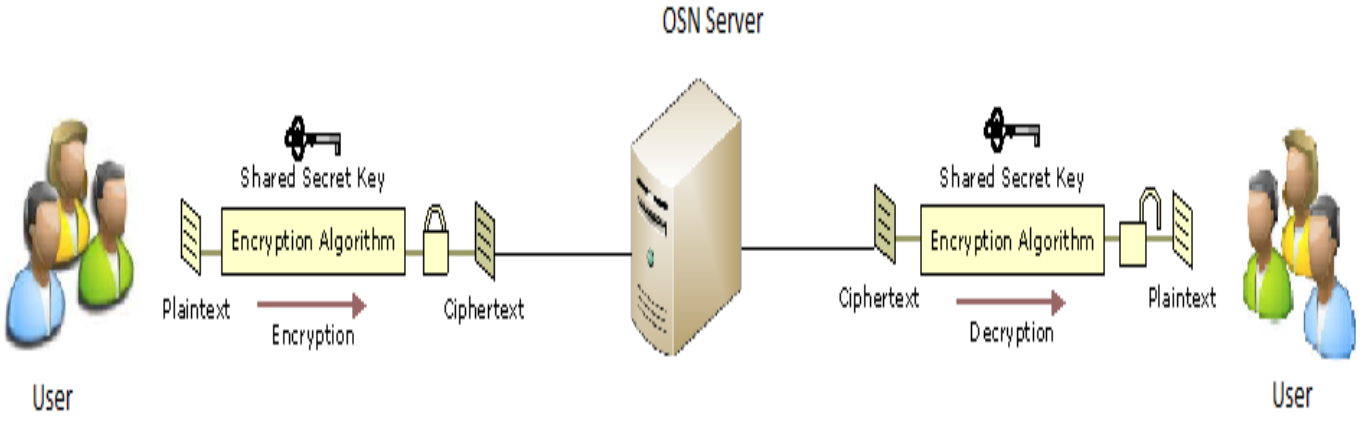

Figure 2: User Privacy Protection Mechanism in Online Social Networks

- When someone needs to impart assets to others, she builds a group together with a set of trusted companions on an OSN stage by Build Community calculation. At long last, every part gets a group key, which can be utilized to get to, oversee and keep up the assets in this group;
- When a client wishes to get into a group, her companions hold the group key can assign a right to gain entrance consent key (APK) to her by utilizing Delegate Permission calculation;
- If one group part needs to post message and asset into the group, she picks the group key, conjures Upload Resource calculation to encode the asset with her private key, and afterward transmits the scrambled information to the capacity server; and
- Anytime one group part can acquire the scrambled information from the server, and summon Download-Resource calculation to recover the first post or asset by her private key and APK.

As indicated by our portrayal, we authorize access control and key administration at the customer side by a gathering of bit parts. In our building design, we don't have to accept that the framework supervisor is trusted to deal with a private OSN, so that the group can be developed in a self-ruling and synergistic route, without the association of a framework chief. To empower access control through key administration without a framework director, our outline ought to fulfill a few vital security and execution necessities, for example, self-rule, freedom, joint effort, confirmation, and repudiation.

Algorithm

Upload-Resource (*ui*, *F*):
1: $u \leftrightarrow SNP$: $b \leftarrow FAthenticate$ (*ui*, *SNP*);
2: **if** *b* is true **then**
3: *ui*: $C \leftarrow Encrypt$ (*ui.sk*, *ui.pm*, *gk*, *F*);
4: $ui \rightarrow SNP$: *C*;
5: $SNP \rightarrow CSP$: upload (*C*);
6: **end if**

Algorithm

Download-Resources (*ui*, *R*):
1: *ui*: $F \leftarrow Decrypt$ (*ui.sk*, *ui.pm*, *R*)
2: *ui*: $b \leftarrow CV erify$ (*F*, *R*)
3: **if** *c* is true **then**
4: *ui*: Message is intact and output *DR*
5: **end if**

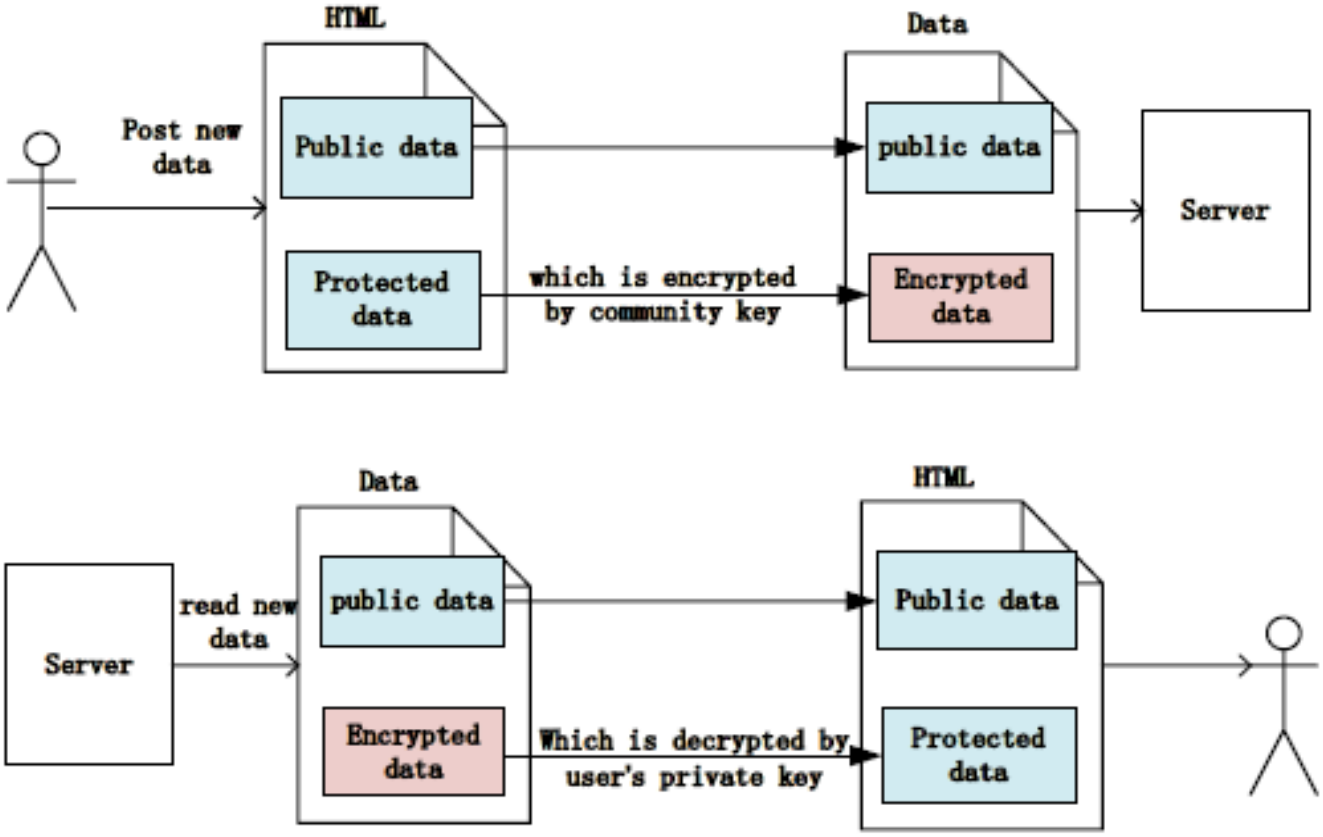

Figure 2: Secure File Sharing System (SFSS) Architecture

IMPLEMENTATION

Directory structure of the Facebook application is very simple and intuitive. Home, upload, download page is on root directory. While Facebook SDK is in "Facebook" directory, Header, footer, style sheets, JavaScript files and images are in their respected directories. Files uploaded by the users are put in "Files" directory which are encrypted form (See Fig 3).

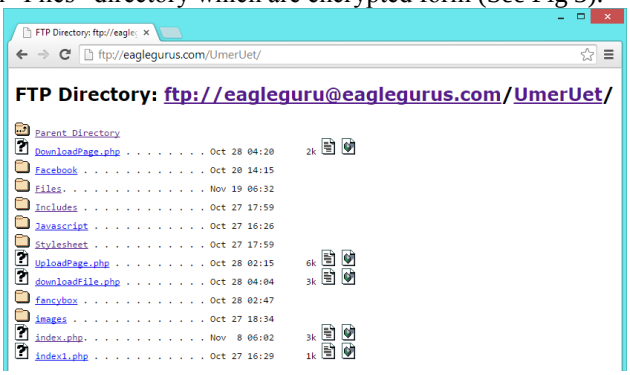

Figure 3: Directory structure of our Facebook application

Figure 4 provides the file sharing app front end that describes that what actions are you may perform through this secure file sharing app.

Figure 4: File Sharing App Front End

Figure 5 provides the file sharing app dialogue box to select the file form any directory and then press upload button to upload and file having image format or doc, pdf etc.

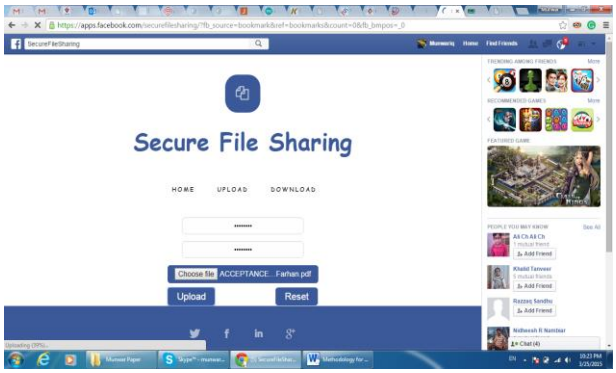

Figure 5: File Uploading and Password Interface

Figure 6 provides the file sharing app message box which confirm that file is uploaded successfully and provide the information that are required to download uploaded file at Facebook.

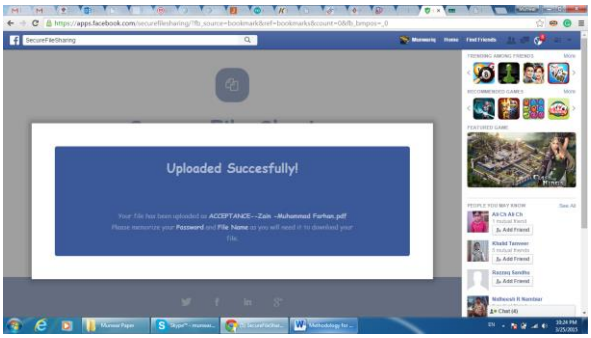

Figure 6: File Uploading Confirmation Message

Figure 7 provides the file sharing app dialogue box to enter the file that you want to download from Facebook. User must enter the file name and password that is noted and shared by the Facebook user who uploaded the file for his friend. This file is out of bound without name and password from other users.

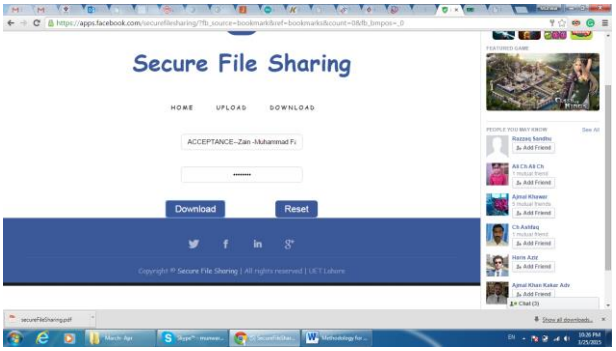

Figure 6: File Downloading Interface.

CONCLUSION AND FUTURE WORK

Users of the OSNs are always experiences the problems with content sharing on OSN network by keep it secure and private. Web brought about the revolution and enormously increases the usage of internet in last two decades. Moreover, the Online Social Networks dramatically becomes prevalent these days. OSNs attracted millions of people and provide them the unique platform to enhance their social circle all over the globe, by sharing their views, photographs, videos, etc. At the same time, various security and privacy issues arise, as all users' personal and private information is in the hands of the OSN providers and can be breached very easily by them or by some other unauthorized access. In this paper we proposed the cryptographic framework to implement the OSN user's privacy. It keeps the files in encrypted form as long as these are in the territory of the OSN providers, thus eliminates the risk of unauthorized access. The authorized users can then download and decrypt these files using the authenticated key. This research provide platform to develop a basic Facebook Application based on our proposed framework, as a proof of concept. We have a plan to go

further deep and explore some more interesting facts about the privacy issues in OSNs and also suggest more effective solutions. User on the other OSNs also face the file sharing is insecure and no privacy application and gadgets are exists. In future work will cover the other OSNs network more effectively and efficiently.

REFERENCES

[1] Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011, November). Analyzing facebook privacy settings: user expectations vs. reality. InProceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference (pp. 61-70).

[2] Beato, F., Ion, I., Čapkun, S., Preneel, B., & Langheinrich, M. (2013, February). For some eyes only: protecting online information sharing. In Proceedings of the third ACM conference on Data and application security and privacy (pp. 1-12).

[3] R. Beale and A. Wood, "Agent-based interaction", in proc. People and Computers IX: proceedings of HCl'94, Glasgow, UK, 1994, pp.239-245

[4] Munindar P. Singh, North Carolina State University, Agent CommunicationLanguages: Rethinking the Principles, http://www.csc.ncsu.edu/faculty/mpsingh/papers/mas/computer-acl-98.pdf

[5] Yanis Labrou, Tim finin and Yun Peng., The Current landscape of Agent Communication Languages, Laboratory for Advanced Information Technology, Computer Science and Electrical Engineering Department, University of Maryland, Baltimore Country.

[6] Aslam Muhammad, Tariq Pervez Muhammad, Mushtaq Seemal, S. Shah Muhammad, Martinez Enriquez A. M., "FMSIND: A Framework of Multi-Agent Systems Interaction during Natural Disaster", In. journal of American Science (Indexed in ISI Master List), Published by Marsland Press, Lansing, USA, MI 48909, ISSN: 1545-1003 **vol. 6**(5), pp. 217-224, May, 2010.

[7] N.K.Nagwani: Performance measurement analysis for Multi Agent System 978-1-4244-4711-4/09/$25.00 ©2009 IEEE.

[8] Tumer PJ. and Jennings N.R. 2000. "Improving the scalability of Multi-agent System", In Proceedings of 4'h International Conference on Autonomous Agents. 2000.

[9] Facebook statement of rights and responsibilities. http://www.facebook.com/press/info.php?statistics# /terms.php?ref=pf.

[10] W. Luo, Q. Xie, and U. Hengartner, "Facecloak: An architecture for user privacy on social networking sites", in CSE (3). IEEE Computer Society, 2009, pp. 26–33.

[11] M. M. Lucas and N. Borisov, "Flybynight: mitigating the privacy risks of social networking" in SOUPS, ser. ACM International Conference Proceeding Series, L. F. Cranor, Ed. ACM, 2009.

[12] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, "Persona: an online social network with user-defined privacy", in SIGCOMM, P. Rodriguez, E. W. Biersack, K. Papagiannaki, and L. Rizzo, Eds. ACM, 2009, pp. 135–146.

[13] B. Carminati, E. Ferrari, and A. Perego, "Private relationships in social networks", in ICDE Workshops. IEEE Computer Society, 2007, pp. 163–171.

[14] S. Guha, K. Tang, and P. Francis, "Noyb: privacy in online social networks", Proceedings of the first workshop on online social networks, pp. 49–54, 2008.

[15] B. Carminati and E. Ferrari, "Privacy-aware collaborative access control in web-based social networks", in DBSec, ser. Lecture Notes in Computer Science, V. Atluri, Ed., **vol. 5094**. Springer, 2008, pp. 81–96.

[16] J. Domingo-Ferrer, "A public-key protocol for social networks with private relationships", in MDAI, ser. Lecture Notes in Computer Science, V. Torra, Y. Narukawa, and Y. Yoshida, Eds., **vol. 4617**. Springer, 2007, pp. 373–379.

[17] J. Domingo-Ferrer, A. Viejo, F. Seb´e, and ´U. Gonz´alez-Nicol´as, "Privacy homomorphisms for social networks with private relationships", Computer Networks, **vol. 52**, no. 15, pp. 3007–3016, 2008.

[18] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, G. Pelosi, and P. Samarati, "Preserving confidentiality of security policies in data outsourcing", in WPES, 2008, pp. 75–84.

[19] K. B. Frikken and P. Srinnivas, "Key allocation schemes for private social networks", in Proceedings of the 8th ACM workshop on Privacy in the electronic society, 2009, pp. 11–20.

[20] B. Carminati, E. Ferrari, and A. Perego, "Rule-based access control for social networks", in OTM Workshops (2), ser. Lecture Notes in Computer Science, R. Meersman, Z. Tari, and P. Herrero, Eds., **vol. 4278**. Springer, 2006, pp. 1734–1744.

[21] V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attribute-based encryption for fine-grained access control of encrypted data", in ACM Conference on Computer and Communications Security, 2006, pp. 89–98.

[22] B. Carminati, E. Ferrari, and A. Perego, "Enforcing access control in web-based social networks", ACM Trans. Inf. Syst. Secur., **vol. 13**, no. 1, 2009.

[23] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and efficient key management for access hierarchies", ACM Trans. Inf. Syst. Secur., **vol. 12**, no. 3, 2009.

[24] G. Ateniese, A. D. Santis, A. L. Ferrara, and B. Masucci, "Provably-secure time-bound hierarchical key assignment schemes", in ACM Conference on Computer and Communications Security, A. Juels, R. N. Wright,

and S. D. C. di Vimercati, Eds. ACM, 2006, pp. 288–297.

[25] M. M. Lucas and N. Borisov, "Flybynight: mitigating the privacy risks of social networking", in WPES, V. Atluri and M. Winslett, Eds. ACM, 2008, pp. 1–8.

[26] Yasir Saleem, M. M. Iqbal, et.al., High Security and Privacy in Cloud Computing Paradigm through Single Sign On. Life Sci J 2012; **9**(4): pp. 627-636.

[27] Kaleem Razzaq Malik, Muhammad Umar Chaudhry, Muhammad Munwar Iqbal, and Et al., "Data Security and Privacy in Cloud Computing: Threat Level Indications", Sci.Int (Lahore), **Vol. 26**(5), pp. 1991-1996, 2014.