International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Data confidentiality in Online Social Networks: A Survey

Vedashree K. Takalkar[1], P N.Mahalle[2]

[1]Savitribai Phule Pune University, Smt Kashibai Navale College of Engineering, Vadgaon, Pune, India

[2]Savitribai Phule Pune University, Smt Kashibai Navale College of Engineering, Vadgaon, Pune, India

Abstract: ***The use of online social network (OSN) has been growing exponentially in the present era. As large volume of data is being uploaded by different users, securing the data from unwanted users is a major issue. The data uploaded on the social networks is not secured according to the policies and requirements of the owner who has uploaded the data. Various factors can be considered to achieve the access control of the data in OSN through different mechanism. The paper surveys these methods rigorously and also proposes the innovative method to achieve data confidentiality in OS by defining the access control mechanisms.***

Keywords: access control, data confidentiality, online social networks, trust based access.

1. Introduction

Being a social animal, it is the tendency of the man to establish the social relationships and enhance the social circle. As the technology has advanced, the same task is now done through OSN. OSN is a dais where people share their data in the form of photos, videos, comments, status updates and so on. OSN user creates his own identity in the social network through his profile. He can establish these links with different users called as friends, mutual friends, friend-of-friend and even tend to accept the friend requests of the unknown people who then may become good friends. Through this links people can get connected to all the people around the globe. To enjoy these benefits of OSN, the popularity of OSN is growing at a large pace. Facebook statistics show that there are about [20] 3.17 billion active users. However, when it comes to the privacy concerns regarding the data that is being uploaded, there is lot of ignorance from the users that may lead to data confidentiality attack. 69.4% [5] users keep their posts public and 7.7% [5] people don't even know if their posts are public or private. All these observations are made from the survey of 325 users that was carried out in [5].These figures conclude that majority of the OSN users are not aware of the issues and problems that may arise if the sensitive data is revealed to the unintended people. When the OSN user uploads the data, he may not want it to be disclosed to certain friends. Hence, there should be some policies that must be defined for each data that is uploaded. Hence, the access control to the data must be given to the friends of the user depending on the some parameters or metrics that will defines the policies for the access control.

The architecture of OSN is shown in Figure 1. This is a layered architecture that focuses on the features that are provided by the OSN for its users. Also it defines different layer at which the functions are performed. The base layer is that of OSN service provider which provides the user facilities to upload data, share data, data repository or data centre where the uploaded data gets stored. Facebook is an example of OSN service provider. The second layer is the layer which holds the relationship data. This is the important layer since it stores the relationship information like friend-of friend, close friend, colleagues etc. This data is used for the access control of the data. This means that OSN has a feature that the data is shown to only the friends or can also be made public. The third layer contains user profiles that reveal who the users are and the data can be further used to analyze the interests of the users. The top most layer contains third party applications that contain the apps that are designed and developed by the third party organizations but can be used by the users on the OSN.

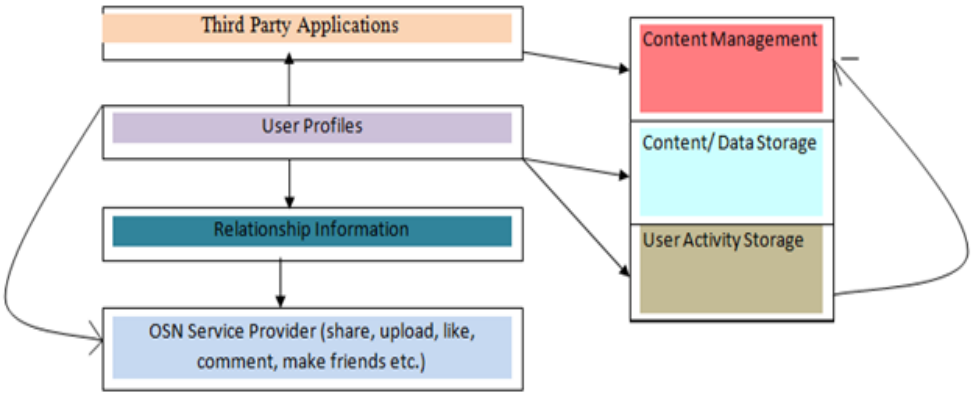

Figure 1: High Level View of OSN

The content management, storage and tracking the user activity (Activity logs in Facebook) are also vital components of the OSN architecture. These layers are the overview of the architecture and can be detailed further. The arrows between the layers show the interaction between the different layers.

Figure 2 details the actions the user performs in OSN. Alice and Bob are the two friends in the OSN. They can upload the different kind of digital data like video, photo etc. and also can share the data. Hence, all friends can interact with each other and also share each other's data. Like Bob anybody can store the data and share the friend's data without any policies that are defined.

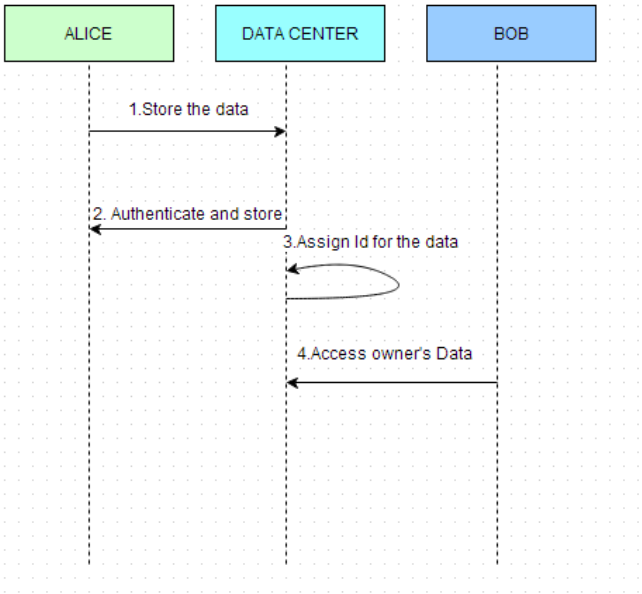

Figure 2: Work Flow actions of user in OSN

2. Motivation

The growing popularity of OSN and increasing users are the main cause for which the access control mechanisms are needed to be imposed. Consider a scenario where Alice, does not want her photo of a family outing to be viewed by some friends in her friend list. Every time to create different lists of people who can access the photo differently is very cumbersome task. Hence, some automated policies should be able to be defined that can be able to do the same task of access control. Also the decision of access control should consist of user opinion as well as the system calculations. Also allowing the sharing of data in a random manner can cause data confidentiality attack on the secured data as the data can then be viewed by the unintended people.

3. Related Work

The popularity of OSN is increasing day by day. [15] was studied to understand the usage patterns of OSN and the extents to which they are used. Growing content on OSN has compelled securing the data to be viewed by the unintended people. The rigorous survey was carried out to study different areas in which the security needs to be increased.[5],[9],[11] are studied to understand the overall domains where the security and confidentiality needs to be increased. The studied work also defines the privacy breaches and mechanisms to defend these breaches. Safebook also works on real life trust with no particular protocol definition. In [12], protocols are defined for batch authentication. They include hash based, proxy based and certification based encryption protocols. They are used to authenticate the user in the groups. As the number of the users in OSN has been reached up high, ensuring the security has been a challenging task. In [1] the author has described the access control methods and mechanisms. The user can mention access policy for every data that has been uploaded by him. Also the disseminator can mention his own access policies. In the multiparty environment, resolving the conflict between the policies related to various users like owner, disseminator and contributor is important and various efficient methods are mentioned. However, there is need for automated policy generation as data uploaded everyday by the user is quite large and assigning the policy for every data always will become cumbersome for the user. Also no trust was taken into consideration between the users. This should be considered in the MPAC policy as trust will decide the strength of relationship between the users which will in turn decide what level of secured data can be allowed to be seen. Considering the trust level is important and should play a vital role in giving the access of the data. More the secured the data is, it should be viewed by only the trusted friends of the user.

However, the trust should be calculated depending on some parameters or metrics.[14] introduces the metric of credibility and reliability among the peer nodes to calculate the trust amongst them. The interactions amongst them are considered to calculate the trust between them. These interactions consist of the messages as well as tags that a user shares with his peer that is friends. However, the interactions cannot alone determine the trust value effectively. [10] also defines the distance as a parameter. To evaluate trust and based on this trust calculation the filtration of the content is done. This is done by using hop based technique and the numbers of hops decide the trust between the user and his friends, however, it does not consider the opinion of the user in deciding the trust score. It also mentions the clustering mechanisms to evaluate trust.

In [5] different methods to calculate trust were defined. They consist of machine based, statistical, heuristic and behavioral. [13] uses a new algorithm to evaluate trust in OSNs using the probabilistic sampling methods.[14] discusses finding of optimal trust path in OSN using heuristic techniques.

These literatures were studied to do the comparison of the current security trends in OSN as well use of trust in OSN. The related work as shown in Table 1 was evaluated to compare the current mechanisms to achieve security. The work was evaluated on parameters like whether the fine grained access was given or not, whether trust is considered or not, id data confidentiality is achieved, and different types of attack that are possible. It also considers the backward and forward secrecy. Hence, the literature below was studied in order to understand the overall security mechanisms that are applied in current OSNs to achieve data confidentiality.

Table 2 was studied in order study the specific domain of achieving access control of the data using a parameter of trust. Thus this evaluation is specific to a parameter of trust.

As shown in Table 2 trust was calculated by different mechanisms and also was used also for other purposes that access control. Also, this evaluation is specific to the proposed work that is mentioned in further section 4.Table 2 evaluates the related work with different parameters like different techniques used to calculate trust. Also it studies if the calculated trust is used for access control or for any other purpose. Hence, it overall studies how the trust value is calculated and how it is used. This does the rigorous survey on the existing methods for trust calculation. Hence, Table 1 is the general literature survey evaluation and Table 2 demonstrates the evaluation for the specific parameter called trust.

Table 1: Overall Evaluation of Related Work

Paper	Trust	Fine grained	Scalability	Key	User revocation	Data confidentiality	Collusion Attack	Backward/forward secrecy Attack
1	No	Not considered	Not Efficiently	No	Not considered	Yes	No	No
2	No	Yes	Yes	ABE	Immediate attribute revocation used	Yes	Yes	Yes
3	No	Not considered (among the users)	Yes	CPABE+PKI	Yes	Yes	Yes	Yes
4	No	Yes	Yes	KPABE+PRE +lazyencryption	Yes	Yes	No	Yes
6	No	Yes	Yes	No	No	Yes but limited	---------	No
7	Yes	Yes	No	Yes (threshold encryption)	No	No	Yes	No
8	No	Yes	Yes	KPABE	No	Yes	No	No

4. Proposed Work

After the rigorous survey, a need was observed to apply the trust based access control in the OSN architecture. As seen from Table 2, trust is not much used for the access control. Also trust must contain the user opinion as well as some characteristics that are derived from the relationship characteristics in the OSN. Every user has friends in his friend list who can view the data uploaded by the user. However, user has a different amount of trust for every friend he has. Some are known while some are not very familiar. The proposed work calculates the trust based on the parameters which are from user considerations as well the system observations. We consider the experience of the user with the particular friend. Also we consider the interactions as mentioned in [14]. Also another innovative addition to the parameter list is about information about how dynamic the friend is on the OSN. As users don't like the friends who are not active in OSN [20], they tend to unfriend the inactive person Hence all these factors together can help in calculating the trust. The trust is hence, the value that is calculated from the combined input of the user as well as the system observations of OSN.

Table 2: Specific Evaluation of Related work (considering Trust parameter)

Reference	Technique used to achieve trust	Is Trust used for Access control?	User opinion considered?	Consideration of Characteristics of friends in OSN
Estimating trust value: A social network perspective[10]	Clustering methods, user generated ratings	No	Yes	No
New Algorithm for Trust Inference in Social Networks [13]	Probabilistic models	No	No	No
Experimental Analysis on Access Control Using Trust Parameter for Social Network[14]	Interactions between users and friends	Yes	No	No
Propagation Models for Trust and Distrust in Social Networks[16]	Propagation models	No	No	No
Finding the Optimal Social Trust Path [17]	Heuristic algorithms	No	No	No
Multiparty Access Control for Online Social Model and Mechanisms[1]	Trust is not considered	No	No	No
Operators for Propagating Trust and their Evaluation in Social Networks[18]	Trust metrics	No	No	No
trust based approach for protecting user data in social networks[19]	Hop based technique	Yes	No	No
Proposed Scheme	Using experience, Context Information and Interaction	Yes	Yes	Yes

From Table 2 it can be observed that the proposed scheme is the only scheme that considers trust from all the aspects. It considers the experience of the user which is a real life experience outside OSN. Also the system in turn calculates the interaction between a friend and user and also checks how much the user is active. With all this, a consolidated trust value is calculated. A user is able to input his experience about a friend during adding him as a friend at the time of accepting a friend request. The user activity can be noted from time to time to measure how active the user is.
The next aspect is about giving the access control based on the trust value calculated for every friend of the user. Whenever a data is uploaded the user is compelled to set a security level for the data. If the security level is high it is viewed by the trusted people itself. This means that it is viewed by only those people who have high trust value.

There is always a comparison between the security level and the trust that every friend has with the user. Hence, the direct variation is established between the trust value and access to the secured data. After the comparison between these values gives the decision regarding the access or denial of access to the user. Hence, the trust based access control can be achieved

5. Conclusion and Future Work

Ensuring the security and data confidentiality has become vital as the number of people is becoming active on OSN and also the content is growing at an exponential rate. So the mechanisms to secure the data need to be imposed in an effective manner. The current OSN trends do not provide much fine grained access policies to be defined. Also OSNs like Facebook define extreme policies for access control like visible to public, visible to only me. Hence, more efficient policies using trust can prove to be more efficient. The proposed work considers the user opinion about the friend in terms of his real life experience and also on the interaction between the friend and the user. The third metric is the context information that tells how much active the user is on OSN.

The future work deals with detailing the concepts about the metrics and calculating the effect of each on the final trust value. Also developing the OSN application which applies the concept of trust based access in OSN is the future work that can be done

.

References

[1] HongxinHu,Gail-Joon, Jan Jorgensen," Multiparty Access Control for Online Social Model and Mechanisms", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 25, NO. 7, JULY 2013
[2] Hunag Qinglon, MA Zhaofeng, YANG Yixian, NIU Xinxin, FU Jingyi,"Improving security and efficiency for encrypted data inOSN"
[3] JunbeomHur, "Improving security and efficiency in Attribute based Data sharing", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 25, NO. 10, OCTOBER 2013
[4] Shucheng Yu, Cong Wang, KuiRen, and Wenjing Lou," Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", INFOCOM, 2010 Proceedings IEEE DOI: 10.1109/INFCOM.2010.5462174 Publication Year: 2010
[5] https://www.stonetemple.com/how-are-people-using-facebook/
[6] Mohamed Shehab , Anna Squicciarini , Gail-JoonAhn ,IriniKokkinou ," Access control for online social networks third party applications",Elseveir 897e911 computers & security 31 (2012)
[7] JunbeomHur," Attribute-Based Secure Data Sharing with Hidden Policies in Smart Grid", IEEE Transactions On Parallel And Distributed Systems, VOL. 24, NO. 11, NOVEMBER 2013
[8] Vipul Goyal, Cong Wang, KuiRen, Wenjing Lou, "Attribute Based Data Sharing with Attribute Revocation", ASIACCS'10, Beijing, China. Copyright 2010 ACM 978-1-60558-936-7, April 13–16, 2010
[9] Hongyu Gao ; Jun Hu ; Tuo Huang ; Jingnan Wang ; Yan Chen ,"Security Issues in Online Social Networks" Internet Computing, IEEE Volume:15 , Issue: 4 DOI: 10.1109/MIC.2011.50
[10] Wei-Lun Chang & Arleen N. Diaz & Patrick C. K. Hung, 'Estimating trust value: A social network perspective', Springer Science+Business Media New York 2014
[11] XI CHEN AND KATINA MICHAEL "Privacy Issues and Solutions in Social Network Sites",IEEE Technology And Society Magazine,2012
[12] Lo-Yao Yeh, *Member, IEEE*, Yu-Lun Huang, *Member, IEEE*, Anthony D. Joseph, *Member, IEEE*, Shiuhpyng Winston Shieh, *Senior Member, IEEE*, and Woei-Jiunn Tsaur, *Member, IEEE,"*A Batch-Authenticated and Key Agreement Framework for P2P-Based Online Social Networks", IEEE Transactions On Vehicular Technology, Vol. 61, No. 4, May 2012
[13] UgurKuter, Jennifer Golbeck,'SUNNY: A New Algorithm for Trust Inference in Social Networks Using Probabilistic Confidence Models', Copyright _c 2007, Association for the Advancement of Artificial Intelligence (www.aaai.org)
[14] SaumyaOmanakuttan and MadhumitaChatterjee,'Experimental Analysis on Access Control Using Trust Parameter for Social Network', Springer-Verlag Berlin Heidelberg 2014
[15] Duong Van Hieu, Nawaporn Wisitpongphan, and Phayung Meesad, 'Analysis of Factors which Impact Facebook Users' Attitudes and Behaviours using Decision Tree Techniques", 11th JCSSE (International Joint Conference in Computer Science and Software Engineering)
[16] Cai-Nicolas Ziegler and Georg Lausen, 'Propagation Models for Trust and Distrust in Social Networks', 2005 Springer Science + Business Media, Inc. Manufactured in The Netherlands
[17] Guanfeng Liu, Yan Wang, Mehmet A. Orgun, Ee-PengLim,'Finding the Optimal Social Trust Path for the Selection of Trustworthy ServiceProviders in Complex Social Networks', IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 6, NO. 2, APRIL-JUNE 2013

[18] Chung-Wei Hang,Yonghong Wang, Munindar P. Singh,' Operators for Propagating Trust and their Evaluation in Social Networks',2009, International Foundation for Autonomous Agents and Multiagent Systems
[19] WILFRED VILLEGAS, 'A TRUST BASED APPROACH FOR PROTECTING USER DATA IN SOCIAL NETWORKS', CASCON '07 PROCEEDINGS OF THE 2007 CONFERENCE OF THE CENTER FORADVANCED STUDIES ON COLLABORATIVE RESEARCH
[20] http://www.pewinternet.org/2012/02/03/why-most-facebook-users-get-more-than-they-give-2/

Author Profile

Vedashree Kedar Takalkar graduated in Computer Science and Engineering from Pune University, Maharashtra, India in the year 2013. She is currently pursuing Masters in Computer Engineering at Smt. Kashibai Navale College of Engineering, Pune. Her research interests are Online network security. She has also published 1 publication in international Journal.

Parikshit N. Mahalle is PhD from Aalborg university and is IEEE member, ACM member, Life member ISTE and graduated in Computer Engineering from Amravati University, Maharashtra, India in 2000 and received Master in Computer Engineering from Pune University in 2007. From 2000 to 2005, was working as Assistant Professor in Vishwakarma Institute of technology, Pune, India. From August 2005, he is working as Professor and Head in Department of Computer Engineering, STES's Smt. Kashibai Navale College of Engineering, Pune, India. He published **39** research publications at national and international journals and conferences. He has authored 5 books on subjects like Data Structures, Theory of Computations and Programming Languages. He is also the recipient of "Best Faculty Award" by STES and Cognizant Technologies Solutions. He has guided more than 100 plus under-graduate students and 10 plus post-graduate students for projects. His research interests are Algorithms, IoT, Identity Management and Security. He has also delivered invited talk on "Identity Management in IoT" to Symantec Research Lab, Mountain View, California