International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 05, May-2015

Handling Data Confidentiality Attack due to Data Sharing using Trust-based Approach in Online Social Networks

Vedashree K. Takalkar, Parikshit N. Mahalle
Department of Computer Engineering
Smt.Kashibai Navale College of Engineering
Savitribai Phule Pune University, Pune, India

***Abstract*—Online Social Networks (OSNs) are getting popular among all the people around the globe. With the growing popularity, achieving the data confidentiality from the user's perspective is considered to be most important. Though data like photos or videos that are uploaded by the owner of the profile is visible to all the friends, it is not always that the user wants it to be viewed by all the friends in the friend list. To give only selected friends the access to the data, a trust based access control mechanism is proposed which will help achieve data confidentiality. The trust score is dependent on different parameters. The paper takes forward the concept of trust-based access control and also proposes the mechanism to handle the threat to data confidentiality due to sharing of the data by friends. Thus the paper solves the problem of data confidentiality attack in OSN due to sharing of the data. To the best of our knowledge this is the first paper that proposes the solution to the threat using trust between the user and friends that occurs due to dissemination of the data in OSN using trust-based approach.**

***Index Terms*—Trust, data confidentiality, Online Social Networks, trust-based access control, threat handling**

I. INTRODUCTION

OSNs like Facebook, Twitter, LinkedIn are getting popular day-by-day. OSN is a network where the people are connected to each other through links called as relationships and users are represented with their profiles. It is a platform where people connect with each other and share data like photos, videos, etc. Facebook survey says that there are 3.17 [2] billion active users on Facebook and this number is growing at a faster rate. The literature related to the human approach regarding the data that is uploaded was studied. It was found that among the 325 users that were surveyed [2] and [4] that only 19.4% users are concerned about the privacy policies regarding the data. OSN can be viewed as a layered architecture as shown in Fig 1. The first layer at the top is third party applications that are available on the social networking sites. These third party applications provide add on facilities to the user. The next layer is user profiles. All the users in OSN are identified by the user profile. It contains all the data related to the user like his name, photo, education, interests, etc. The relationship information is stored in the next layer which tells about the relations between different OSN users. It will contain the information like who is whose friend and so on. The last layer is of OSN service provider which provides different services like uploading the data, commenting, liking etc. All these are the basic facilities provided by the OSN provider. OSN provider is responsible to provide all these facilities as mentioned in [5].

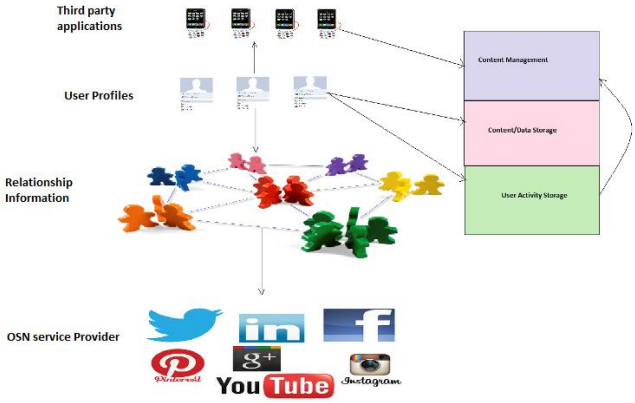

Fig 1 Generalized View of OSN

II. MOTIVATION

Considering the present scenario, the access control policies that are available are not much effective and flexible [6]. They either allow you to keep the data on the OSN or delete it which is a binary decision and is not much flexible. User Alice has uploaded a photo which she wants to share with only selected friends in her friend list. Hence, she wants her photo to be accessed by only trusted people or the friends whom she trusts more. Hence, she wants an automated mechanism that is able to select the trusted friends from the friend list. Alice expects that the decision of access control should be based on the metrics derived from the system calculations as well as the user considerations also. Hence, user's efforts of selecting the friends like in current scenario will be reduced and the task of selective access control is simplified.

III. RELATED WORK AND EVALUATION

TABLE I OVERALL EVALUATION OF RELATED WORK [1]

Reference	Trust	Fine Grained	Scalability	Key	User revocation	Data confidentiality	Collusion Attack	Backward /Forward Secrecy
Multiparty Access control for Online Social models and mechanisms[2]	No	No	Not efficiently	Not used	No	Yes	No	No
Improving security and efficiency for encrypted data in OSN[3]	No	Yes	Yes	ABE	Immediate attribute Revocation	Yes	Yes	Yes
Improving security and efficiency in Attribute based data sharing[4]	No	no	Yes	CPABE +PKI	Yes	Yes	Yes	Yes
Achieving Fine-grained data access control in cloud computing[5]	No	Yes	Yes	KPABE +PRE	Yes	Yes	No	Yes
Access control for online social networks third party applications[6]	No	Yes	Yes	No	No	Yes but limited	----------	No
Attribute based data sharing with hidden policies in smart grid[7]	Yes	Yes	No	Yes	No	No	Yes	No
Attribute based data sharing with attribute revocation[8]	No	Yes	Yes	KPABE	No	Yes	No	No

The literature was studied to understand the current scenario in the OSN as far as data confidentiality is concerned. The literature was studied to understand the privacy and security issues [5], [7] in OSN. They were studied to understand the overall security risks and proposed solutions to them. The other literature was studied to understand the use of trust in OSN. The comparison of different literature survey as in [1] shows the use of trust in OSN. The conclusion from the study states that though trust was used in OSN it was not much applied for access control of the data.

The literature was studied with respect to the factors like data confidentiality, key used in case of security, user revocation, use of trust, scalability, use of fine-grained access control is used, the attacks that are considered and so on.

Table2 as mentioned in [1] studies the specific literature from the point of view of trust and its use in access control of the data. Hence two types of study were conducted. One was specific to the proposed work and the other was a general study to understand the current scenario with respect to data confidentiality in OSN.

TABLE II SPECIFIC EVALUATION OF RELATED WORK(CONSIDERING TRUST) [1]

Reference	Technique used to achieve trust	Is Trust used for Access control ?	User opinion considered?	Consideration of Characteristics of friends in OSN
Multiparty Access Control for Online Social Model and Mechanisms[2]	Trust is not considered	No	No	No
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
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

IV. PROPOSED WORK

Considering the current scenario, the access control mechanisms that are proposed pose cumbersome issues with respect to the user friendliness. Hence, the proposed method considers the access control with respect to trust derived from specific parameters like experience, context information and

interaction between the friends in the OSN. This also includes the access control rule that allows only the access of secured data to the friends those have higher trust value. Here, the trust score calculation is based on the input from the owner as well as some system derived conclusions. Solely relying on either system or the user input may not prove efficient. Hence, the final decision of access is the blend of the owner input as well as the system calculations. Experience is a parameter which is taken as a user input. Context information states about the dynamicity of the friend on the OSN. It says how much active the person is on OSN. The interaction considers how much interaction is there between the owner of the profile and the friend. Accordingly the credibility as mentioned in [14] is calculated. All these factors are considered to calculate the trust score.

A. Responsibilities of Trust System

- Maintaining the data

The data center stores all the data like photos, videos uploaded by the user. The data id is generated to identify each data uniquely.

- Tracking of user Activity

This is required to track the user activity like number of times user has changed the profile picture, number of times he has logged in, number of posts posted by a particular user. These counts are maintained in order to know the dynamicity of the user. Number of friends is also taken into consideration while calculating the context information.

- Managing the Trust scores

As mentioned earlier, the trust score is calculated from the experience, context information and interaction between the user and friends. The trust scores are calculated and updated if required with dynamic values that are considered.

- Making Decision of Access or Deny

To allow access of the data to a particular friend of the user will depend on the trust score that has been calculated by the system. A user assigns a security level as mentioned in [2].Those friends who have trust score more than or equal to the security level are allowed to see the data like a photo or video. However, those who fail to achieve this criteria are denied the access.

B. Handling Threat to Data Confidentiality

The problem of access control occurs especially when the friends share your data abruptly. Once, the data is shared there remains no control over the data like photos and they can be viewed by anyone. This problem can be coined as revelation of information due to dissemination. Different methods as mentioned in [2] were studied. However, these mechanisms involve lot of user intervention which is not an effective mechanism. Some automatic mechanism needs to be proposed in this direction. The proposed threat model implements voting scheme for the access control decision. As mentioned in [2], the voting mechanism considers the decision of each and every person who is tagged in the particular post or a photo. Voting scheme contains trust-based voting mechanism. Here, the voting will consider the trust that is already calculated.

Consider a scenario where the owner O uploads the photo and tags n friends $\{f_1, f_2, \ldots\ldots, f_n\}$.The proposed trust-based voting mechanism says that the final trust score is calculated which is an aggregated trust score values from all n friends and O.

Suppose f_j shares a photo uploaded by O then the aggregate trust score is calculated depending on the trust score value each one in the set $\{f_1, f_2, \ldots\ldots, f_n\}$ and O has for f_j. Suppose f_i from the set is not a friend with f_j then in that case $T_{fi->fj}$ is 0. Like wise the aggregated trust score is calculated depending on the trust scores of all stakeholders.

$$Tsc = \frac{To + \sum_{i=1}^{n} Tfi \rightarrow fj}{n} \quad (1)$$

After the aggregated trust score is calculated the T_{sc} is compared with threshold value that has been initially given by O while uploading the photo. This threshold value is also called as security level. As mentioned in [2] every data like photo when uploaded have some security level attached to it which is given by the owner of the data. This tells sensitiveness of the data uploaded. If T_{sc} is less than the threshold then f_j is denied access else the access is allowed.

This will help in an access control decision which truly involves the trust score of each and every stakeholder involved in the photo or any data that has been uploaded. This strategy is used for conflict resolution in multiparty access control [2] however, trust was not considered for the same.

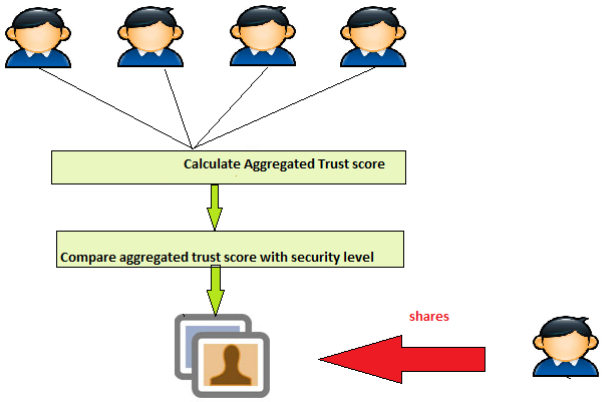

Fig 2 Threat handling Model

V. CONCLUSION AND FUTURE SCOPE

The proposed work deals with the addition of trust attribute in OSN which is not much used in building relationships as well as data access control in current scenarios. Hence, the literature was studied and a trust system from OSN perspective was designed to achieve a trust-based access control.

The future scope lies in defining trust in more dynamic manner and implementing the trust system in suitable technologies. Also, future work aims at collecting the result samples from real time trust system and evaluates the trust-based access control against the different models that are used for the access control in OSN currently.

REFERENCES

[1] Vedashree Takalkar,PN.Mahalle," Data confidentiality in Online Social Networks: A Survey",IJSR,Vol 4 issue 1 Jan 2015

[2] 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

[3] Hunag Qinglon, MA Zhaofeng, YANG Yixian, NIU Xinxin, FU Jingyi,"Improving security and efficiency for encrypted data in OSN" Communications,China Volume 11, Issue:DOI: 10.1109/CC.2014.6825263 Publication Year: 2014

[4] JunbeomHur, "Improving security and efficiency in attribute based data sharing", IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 10, October 2013

[5] 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

[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] 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] Saumya Omanakuttan 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 Service Providers 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 Multiagen tSystems

[19] Wilfred Villegas, 'A Trust Based Approach For Protecting User Data In Social Networks', cascon '07 proceedings of the 2007 conference of the center for advanced studies on collaborative research

[20] http://www.pewinternet.org/2012/02/03/why-most-facebook-users-get-more-than-they-give-2/

[21] http://mashable.com/2011/12/19/friend-unfriend-facebook/