Trust Based Access Control for Social Networks (STBAC)

Saumya Omanakuttan
Department of Information Technology
Pillai's Institute of Information Technology, Navi Mumbai, Maharashtra, India

Madhumita Chatterjee
Department of Computer Engineering
Pillai's Institute of Information Technology, Navi Mumbai, Maharashtra, India

Abstract- The security of our personal information and sharing that information in the digital world has always been a major challenge for the ever-growing social networks. This paper proposes a trust access control called Trust Based Access Control for Social Network, or STBAC, which allows users to share data among their friends, using a trust computation to determine which friends should be given access. This trust computation uses previous interactions among a user's friends to classify his or her peers into privileged or unprivileged zones, which determine whether that peer gains access to the user's data.

Keywords – Trust, trust threshold, credibility and reliability, STBAC

I. INTRODUCTION

Online social networks are currently one of the most popular Internet activities, recently even eclipsing email usage. More than two-thirds of the global on-line population visit and participate in social networks, confirming its worldwide popularity [9]. Online social networking websites leading this trend are Facebook and MySpace, with Facebook presently leading the competitors with impressive usage statistics. The percentage of worldwide Internet users that visit Facebook is reported to be a monthly average of 32%. That amounts to almost one third of all Internet users at a given point. In comparison, MySpace attracts only a monthly average of 3%. Based on these statistics, online social networking is without question, a global phenomenon. Together with such a fast spreading activity, various concerns and risks become evident. The establishment of trust and the protection of users becomes an ongoing challenge within the online social networking environment, with the threat of misuse and privacy intrusions by malicious users illustrating this challenge.

II. MOTIVATION

Online social networks have experienced a surge in popularity recently, particularly because they allow users to share music, photographs, home movies, and blogs with friends and family quickly and easily. The access control mechanism used by these networks to share data is based primarily on relationship depth (friend, friend-of-a-friend, etc.), organization membership (such as a workplace or school), or, as is the case with facebook.com, geographic location (such as a city or country network).

This protection scheme, while straightforward assumes that all friends are equal. Clearly, this is not always the case in real life. These social networks fail to account for the fact that some friends may be more trusted than others. More fine-grained control is needed in the access control mechanisms currently employed by social networks. A simple solution for this problem would be to use access control lists that explicitly denote which users are allowed access to the data. While this approach gives the owner of the data the fine-grained access control we seek, it control that the owner assign access rights to each friend that should see the data. This can be time consuming and repetitive for the owner, and the amount of effort required for data management can scale up as a product of the number of data objects and the owner's friend list. In order to deal with the increasing amount of user-generated data, we must develop protection techniques that minimize the amount of effort required to manage such large volumes of information.

Once the user accepts a person as friend the current social networking site access control decisions do not impact the topology of the social network which is often not valid. For example Alice must be interested to share some data with Bob but not with Ron, this is due to lack of trust Alice has over Ron but in ongoing social network there is no solution for the impact

on friendship status. All the setting in any social networks is static in nature but in real life the status of friendship is very dynamic in nature, this can impact the user's desire for certain friends to access his or her data at certain times.
We proposed a system Trust based Access Control for Social Networks (STBAC) which evaluates the user's friendship status on the parameter of trust with respect to time, depending on the user's previous interaction with the user's friend thus making it dynamic in nature, considering the impact of each friendship with the user. As social networks become more popular, they will become an increasingly important method of communication. Because of this, it is of vital importance that we start considering effective and flexible access control scheme to protect the data in social network.

The rest of the paper is organized as follows; proposed system along with its modules is explained in section II. Proposed STBAC calculation and algorithm are explained in section III. Concluding remarks are given in section IV.

III. PROPOSED SYSTEM

We propose a Trust Based Access Control for Social Networks (STBAC), which allows users to share data among their friends, using a trust computation to determine which friends should be given access. Just as in real life relationships, the trust levels can vary from friend to friend, and may change over time.

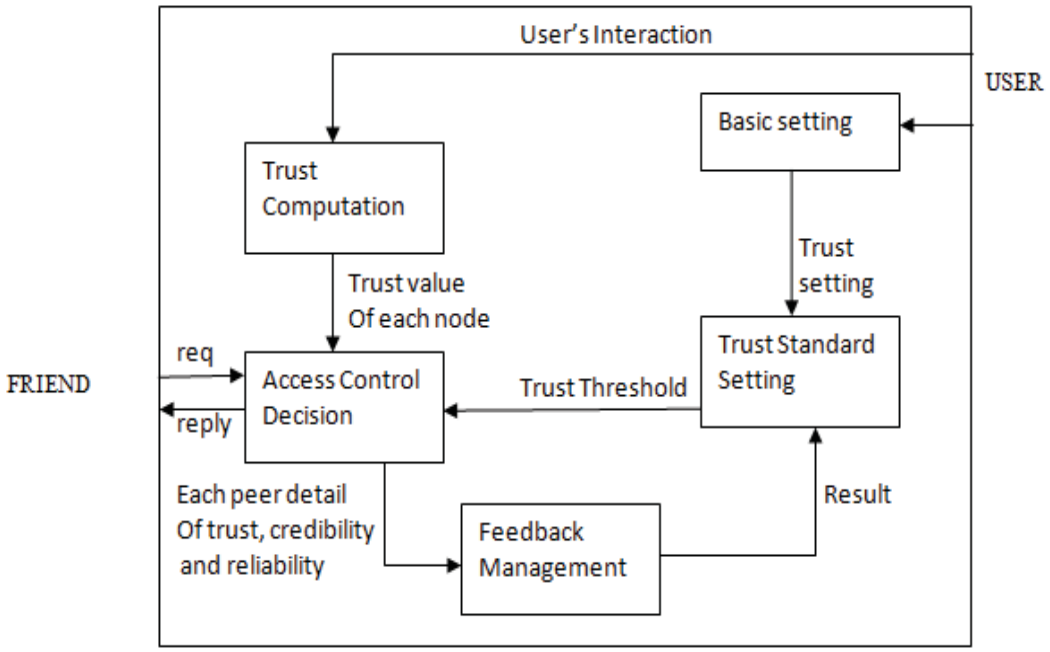

Figure1: The Proposed System for Trust based Access Control for Social Networks (STBAC)

The STBAC is used as a filter in order divide the friends into two broad category of privileged and unprivileged friends where a privileged friend can view all the detail of the user like wall, photos, personal information and can share as well but the unprivileged friend won't be able to view users photos or video as per the user request. This filtration is based on a major concern human parameter, Trust.

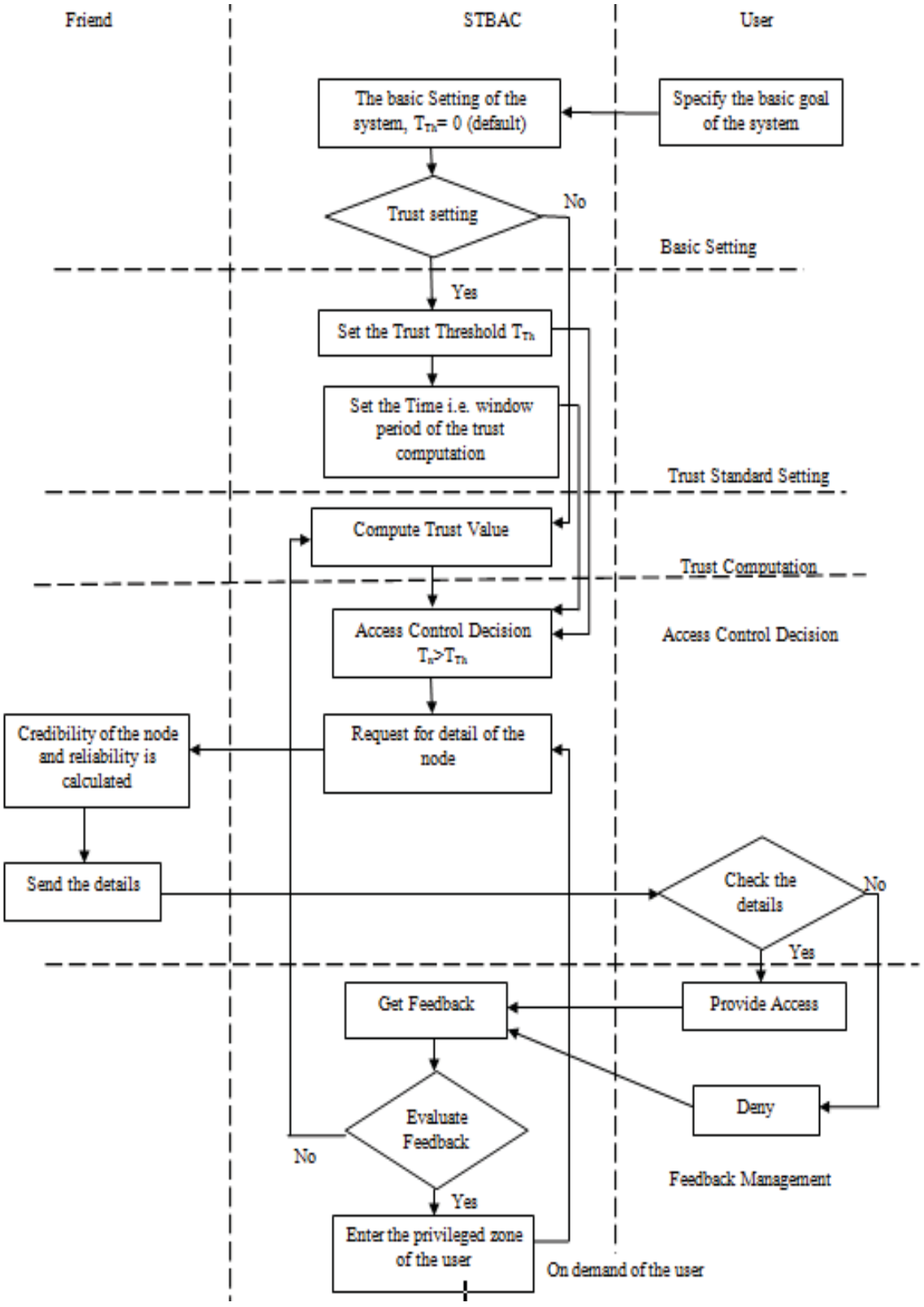

Figure 2: Working of the proposed STBAC

The above figure 1 and 2 describes the proposed system for social networks which consist of two actors involved the user and friend. The entire system consist of major five modules such as basic setting, trust standard setting,

feedback management, access control decision and the trust computation. The STBAC modules thus are explained in detail below

3.1Basic Setting :
The user is suppose to first set a specific goal of using the social networking site i.e. for personal communication with friend or marketing or networking as per the user interest. The user would set its basic account
setting which is static in nature, according to the user's goal the user should decide on whether he or she want the trust setting or not. In case the user select the trust setting then the user would proceed with the trust standard setting otherwise the trust threshold of the user is set to zero (0)
3.2Trust Standard Setting:
In this module the user has requested for the trust setting which deals with two primary setting, the trust threshold and the time. The trust threshold (T_{Th}) is the minimum value the friends need to view the private information of the user. The trust threshold value is set by the user as per how strong they want their private data to be view by their friends. Trust is a parameter which is time dependent. For example a friend who is in the privileged zone now may not be a trusted person after a period of time thus the user need to set the window period for a periodic check on the privileged friends.
3.3 Trust Computation :
The parameter trust of a user is evaluated using the previous interaction of the user with its friends. The different forms of interaction like comment, likes , scraps, tagging , messaging all of these will be incorporated as transaction thus will be used for the calculation of trust value of the friend, credibility of the user and reliability of the user . The trust parameter is calculated on the basis of outgoing transaction with each friend by total number of transaction being performed by all the friends. The credibility of the user is normalized summation of all positive and zero transaction for instance when the incoming transaction of the user is more than outgoing transaction or no transaction with friends. The summation of product of the credibility and trust of each friend node will result the reliability of a node in the networks denoted as R (u,i) where u is the host whose reliability is determined with respect to the friend peer 'i'.
3.4Access Control Decision:
As per the trust computation the trust value of each friend node is compared with the trust threshold value of the user and if the trust value of the friend is greater than the threshold of user then the STBAC send for the request of the friend reliability and credibility details. When user gets this information the user can decide on to whether to accept the friend or reject him/her. In both the case the detail is to the feedback management module.
3.5Feedback Management:
Once the user take a decision on whether to accept the friend in the privileged zone or not the feedback of each friend node is recorded for future reference. The friend whose request is accepted by the user enters the privileged section of the user data but can be reviewed anytime by the user in case required on user demand. If the friend node is denied with access even this will be recorded in the feedback and the friend node will enter the trust computation module with a zero transaction count thus building trust from the beginning.

IV. PROPOSED CALCULATION AND ALGORITHM

4.1 Proposed STBAC Calculation
In a social network trust plays a very vital role. The trust of each peer is calculated on the bases of number of transaction being performed with the neighboring peer or the friend involved in the network. Suppose 'X' is user who has 'n' number of friends thus X will have transaction such as comments, like, message or scrap, sharing of images etc with these nodes. Thus any node trying to perform as of those actions is said to be a transaction which is used to evaluate the credibility of the node and the trust of each node.

4.1.1 Credibility of a peer
Suppose a peer 'u' has 'i' peer as friends or the neighboring peer. Thus performs 'X 'transaction. The incoming transaction is denoted as '$X_{incoming}$' and outgoing transaction with any peer is denoted as '$X_{outgoing}$'. The difference between the incoming and outgoing transaction is denoted as'd'.

$$d= X_{incoming} - X_{outgoing} \quad (1)$$

If d is a positive value implies that the incoming transaction is more than the outgoing transaction of node 'u' thus denoted as 'dp'
If d is a negative value implies the incoming transaction is less than the outgoing transaction of a node 'u' thus denoted as 'dn '.
If d is zero which implies two conditions that either the incoming and outgoing transactions are equal or there is no transaction at all within the peers denoted as 'do'.
Thus credibility (Cr) of a peer is defined as

$$Cr(p(u,i)) = \{\frac{1}{i}\ [\sum dp + \sum do]\} * 100 \qquad (2)$$

If Cr (p (u, i)) > = 75 || 1
Otherwise || 0

If the Cr(p(u)) is greater than or equal 75% implies than the friend node 'i' assures that the user 'u' has high credibility thus is assigned '1'
If the Cr (p (u)) is less than 75% implies than the friend node 'i'assures that the user 'u' has low credibility thus assigned '0'.

4.2 Trust access of a node.

Trust of a peer is determined on the basis of total number of transaction performed between the peer and its friends. Suppose 'u' has n number of transaction with another peer 'v'. Thus trust (T) of the peer 'u' with respect to 'v' will be calculated as follows.

$$T(p(u,v)) = \frac{\sum outgoing(p(v))}{\sum p(u,i)} * 100 \qquad (3)$$

$T(p(u,v)) >= T_{Th}$ || Allow access
Otherwise || Access denied
Where
p (u,v)= transaction between the user 'u' and a friend node 'v'
p (u,i)= total number of transaction of u with all the friend node 'i' in the social network
p (v)= friend node 'v'
$X_{outgoing}$ = Outgoing transaction
T_{Th} = Trust Threshold which is input as per the user.
If the trust value of p(u,v) is greater than the set T_{Th} then the friend node 'v' should be able to access all the private data such as photos document of a person else the access should be blocked.

4.3 Reliability of a node:

The summation of product of the credibility and trust of each friend node will result the reliability of a node in the networks denoted as R(u,i) where u is the host whose reliability is determined with respect to the friend peer 'i' in the network thus calculated as follows.

$$R(u,i) = \sum_{i=1}^{N} T(p(u,i)) * Cr(i) \qquad (4)$$

Where T(p(u,i)) is trust value of each peer and Cr(i) is the credibility of a peer. Thus we can check the reliability of a user thus results a reduction in the dummy node. Thus the above three trust parameter is purely time dependent as per the user interest. Thus the evaluation of the system will result in the better access system for social networks

B Proposed Algorithm for STBAC

Input: u // u is the user
for v=1 to n do
Retrieve Feedback (v, win) // v is peer with whom node u is interacting for 'win' window period

T^0(v) -------- default // set the trust value
end for

Repeat for v=1 to N do
T^{i+1} (v) // Compute trust for each peer from eq^n (3)
end for

// feedback
for i = 1 to length
p(u,i) <= feedback source of feedback(i)
if Cr_T(p(u,i)) != Null then
Cr(p(u,i)) <= Cr_T(p (u,i))
else
Cr(p(u,i)) < = $T_{default}$
end if
end for

// for time of Trust level
T(u) // trust for default
Ts(u) // Trust for a window time thus forming a subset
If T(u) – Ts(u) > $T_{Threshold}$ then
T(u) <= Ts(u)
else
T(u) <= $T_{default}$
end if

V.CONCLUSION

Thus our proposed trust based access control for social network (STBAC) allows user to differentiate among his or her friends in the social network, dynamically. STBAC also help user to identify the malicious peer via a credibility and reliability parameter for each peer, thus reducing the dummy node. As social networks become more popular, they will become an increasingly important method of communication. Because of this, it is of vital importance that we start considering effective and flexible access control scheme to protect the data in social network.

REFERENCES

[1] Xiaoning Ma; Zhiyong Feng; Chao Xu; Jiafang Wang; , "A Trust-Based Access Control with Feedback," *Information Processing (ISIP), 2008 International Symposiums on* , vol., no., pp.510-514, 23-25 May 2008

[2] Ran Yang; Chuang Lin; Yixin Jiang; Xiaowen Chu; , "Trust Based Access Control in Infrastructure-Centric Environment," *Communications (ICC), 2011 IEEE International Conference on* , vol., no., pp.1-5, 5-9 June 2011

[3] Poniszewska-Maranda, A.; , "Platform for Access Control Management in Information System Based on Extended RBAC Model," *Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 2010 12th International Symposium on* , vol., no., pp.510-517, 23-26 Sept. 2010

[4] B. Lampson, "Protection," in Proceedings of the 5th Annual Princeton Conference on Information Sciences and Systems, (Princeton University), pp. 437-443, 1971

[5] M. Benantar, Access Control Systems: Security, Identity Management and Trust Models. New York, NY: Springer, 2006

[6] D. E. Bell and L. J. LaPadula, "Secure computer systems: Mathematical foundations," Tech. Rep. MTR-2547, The MITRE Corporation, Bedford, MA, Mar.1973.

[7] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," IEEE Computer, vol. 29, no. 2, pp. 38-47, 1996.

[8] B. Carminati, E. Ferrari, and A. Perego, "Rule-based access control for social networks," in OTM Workshops (2), pp. 1734-1744, 2006.

[9] Galpin, R.; Flowerday, S.V.; , "Online social networks: Enhancing user trust through effective controls and identity management," *Information Security South Africa (ISSA), 2011* , vol., no., pp.1-8, 15-17 Aug. 2011.

[10] Hua Wang; Lili Sun; , "Trust-Involved Access Control in Collaborative Open Social Networks," *Network and System Security (NSS), 2010 4th International Conference on* , vol., no., pp.239-246, 1-3 Sept. 2010

[11] Graffi, K.; Mukherjee, P.; Menges, B.; Hartung, D.; Kovacevic, A.; Steinmetz, R.; , "Practical security in p2p-based social networks," *Local Computer Networks, 2009. LCN 2009. IEEE 34th Conference on* , vol., no., pp.269-272, 20-23 Oct. 2009

[12] Li Xiong; Ling Liu; , "PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities," *Knowledge and Data Engineering, IEEE Transactions on* , vol.16, no.7, pp. 843- 857, July 2004.