Confidentiality in Online Social Networks; A Trust-based Approach

Vedashree K. Takalkar and Parikshit N. Mahalle

Smt. Kashibai Navale college of Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India
Email: vedatakalkar@yahoo.com; aalborg.pnm@gmail.com

Received 2 November 2015; Accepted 4 December 2015;
Publication 22 January 2016

Abstract

Considering the growing popularity of the Online Social Networks, achieving data confidentiality from user's perspective has turned out to be a vital issue. A system using trust can provide access control for the data uploaded by the owner on the social network. The paper discusses various metrics to calculate the trust and evaluation of trust score to determine the trust an owner has with the friends in her social network. Also the paper proposes the architecture that will build this trust evaluation system. Hence, the data will be seen by the friends who are trusted and the motive to achieve data confidentiality is achieved using trust-based access control scheme. The paper also discusses the Trust Rule to achieve access control of the data. To the best of our knowledge, this is the first proposal that calculates trust based on experience, context information and interaction.

Keywords: Online Social Network, trust, trust score, access control, data confidentiality.

1 Introduction

Man is social animal. OSNs (Online Social Networks) are designed and developed for the people around the globe to interact with each other and get connected. This is a platform through which an OSN user develops his

Journal of Cyber Security, Vol. 4, 213–232.
doi: 10.13052/jcsm2245-1439.427

own identity and interacts using this identity sharing his personal and public data with all the people connected to him called as friends. An OSN user gets connected with his friends, colleagues, friends-of-friends, relatives and even unknown people who then might become good friends. Thus OSNs were mainly developed for strengthening the already existing relations and establishing the new relations. To reap such benefits, people are using OSNs like Facebook, Twitter, Myspace, LinkedIn etc. Facebook statistics boasts to have [2] 3.17 billion active users. Thus, this figure explains the usage of the OSN. However, in the above scenario the data that is uploaded needs to be given a secured access. The survey of 325 Facebook [4] users claims that about 69.2% people keep their posts public and 7.7% people don't even know whether their posts are public or private. Also the survey [4] infers that only 19.4% people are concerned about the privacy policies that are used in Facebook. The conclusion from these statistics states that people are not much aware about the hazards and the problems that may be caused if the sensitive data is reached to the unintended users. Hence, some access control policies should be stated by the users for every data that they may upload. For example, if Alice uploads the photo of her family function, maybe she doesn't want it to be seen by the friends who she doesn't know much but still exist in her friend list. However, due to weak privacy concerns this motive is never fulfilled and the photo is accessed by the unintended friends. Also the present OSNs allows us either to keep the data public or private which are the two extreme cases that cannot provide the data confidentiality effectively [5]. Hence, giving access control of the data to the friends should be based upon some criteria. The paper discusses adding the flavour of trust to give access control mechanism. In real world all the relations are established on trust which mainly comes from the knowledge and experience of the person and his behaviour. The paper also discusses about the factors that are considered to calculate the trust among the owner of the profile and his friends. Depending upon the trust that the owner has towards his friends, the access of the data can be given. Thus, depending on this the selective display of data can be given to all the friends of the owner.

The Figure 1 shows the high level view of the OSN architecture. Here, the users shown are nothing but the user profiles that exists in the OSN to identify the real users. The data server is used to store the data uploaded by the users. The OSN provider [10] gives all the facilities that are needed by the OSN users. These services include functionalities like storage, maintenance and access of the data. The users interact with each other, upload data and communicate with each other. The architecture as shown in Figure 1 is a layered architecture of OSN where each layer shows the different tasks that are performed by OSN all

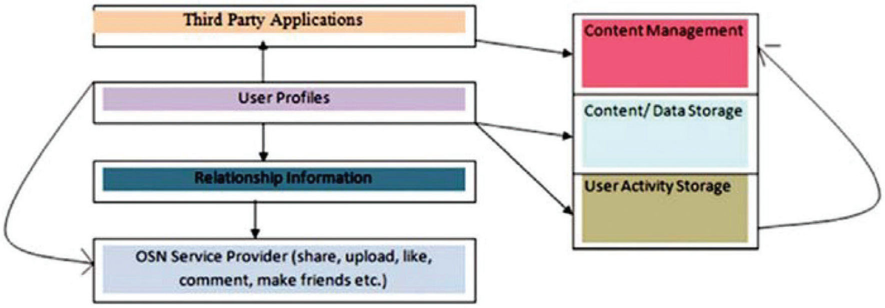

Figure 1 High level view of OSN.

together. On the top are the third party applications that are developed by the third party developers that are installed externally and manually by the users according to their own choice. Next layer is the user profiles which maintain the profiles of all the users. Relationship information is the social link that is shared between different users in the OSNs. It may include the various groups, friend, mutual friend and the other links. The last layer is the basic services that are provided by the OSN provider which are required by the users like sharing, uploading the data, commenting, following, liking, posting etc. These are all the OSN services and hence, act as the foundation for all the above layers. Along with this, all the layers are also dependent on the content manager and content storage. For, this all the data or the content needs to be managed and stored properly. Also, the user activity information is also needed to be stored like who liked which data, who commented on which data, who uploaded on which data etc. Hence, the user activity storage plays a vital role.

2 Motivation

It has been observed that users are not much aware of the privacy features available in OSN [2]. Hence, such ignorance leads to the data confidentiality attack and the secured data is accessed (shared, viewed) by the unintended people. Also, the people in order to increase their friend list tend to accept the friend request of strangers. Observing that the user is from same company and the action of declining the friend request should not hurt the person [11]; users tend to accept the friend request. Hence, all the friends in the friend list are not always the people who are best known or trusted. Hence, whenever any data like photos, status is uploaded owner may not want it to share with the people who exist in friend list but are actually the strangers. Hence, this may cause privacy breach to the highly secured data that has been uploaded by the owner. Trust plays a very important role in the daily life of man. All the transactions of day to day life are based on the real life trust. Hence, sharing of the data can be based on the trust the owner has for the friends in his friend list. Highly secured data is shared with the friends having greater trust.

Alice uploads a photo. She wants it to be seen by the friends who she trusts more as she feels that the data is more secured. It is obvious that the secured data is always shown to the trusted friends. However, she feels that the trust system that provides access control based on the trust value should also consider her opinion about her friends and also the system should consider other metrics such as interaction and dynamicity of the user while sharing the data. Hence, as Alice determines how much the data is sensitive, the system lists all the friends in her friend lists who are allowed to see the photo. Now, Alice's motive of sharing the data with close friends or trusted friends is satisfied.

3 Related Work

As mentioned in [5], the access control policies are designed keeping in mind the security level of the data and then the friends to whom the that data should be shown. However, the trust factor was not considered in the access control. [6] introduces the actual concept of trust in social network by calculating credibility, reliability through the peer interactions. However, more parameters can be considered to calculate trust amongst the owner and his friends. Trust Based Access Control for social networks (STBAC) was proposed which allows the trust computation amongst the owner and his friends and the data is given the access depending upon the trust between the owner and his friends. The interactions like messages and tags that the owner of the profile shares with his friend is the metric that is used to compute the trust value between the owner and friend. However, there is a disadvantage for this metric. The messages or tags cannot alone determine the trust value. Also it may happen that a good old friend may not chat on the social network much. Hence, more metrics are needed to be taken into account in order to make trust computation to be more efficient. Also according to the statistics [4] private messages are not frequently used. Hence, the interaction cannot be considered to be the sole criteria to evaluate the trust score. [7] takes into consideration the distance metric in the social network for determining the trust value and uses this trust value to filter out the content. [7] also uses clustering techniques to evaluate trust. Various techniques that were used in evaluation the trust are mentioned in [5] such as machine-based, behavioural, statistical and heuristic based techniques. [8] discusses various propagation models for trust and classification schemes for trust metrics. Also Appleseed was proposed in [8] to compute trust in local group. In [9] the distance metric is used. Hop based technique is used to decide the trust value between the users in OSNs. Lesser the hop distance more trusted the user is. Hence, in this approach the user's opinion about that particular friend is not considered. Also [12] proposes a new algorithm for trust based inference in social network. It uses probabilistic sampling and hence, calculates the trust for every source in the social network. [13] proposes finding optimal trust path between service provider and service consumer. As there are many social trust paths available, selecting the optimal one is a tough task. [13] proposes different heuristic algorithms to achieve the same. The work in [15] throws light on the pattern of usage of Facebook which tells us the popularity of the OSN sites and the extent to which they are used.

4 Evaluation of Related Work

The above related work was studied to understand the different techniques that are used to calculate the trust between the users in OSN. Each work throws light on the different methods with which the trust was calculated. The works that were studied considered trust for the purposes different than access control like for recommendation systems. Also consideration of user's opinion in the trust calculation is also vital which was not considered by many referred works. Real life trust factor (EX in our case) from the owner's perspective will always prove to be most efficient method to calculate trust.

5 Proposed Work

Considering the literature survey that is done, it is concluded that not much work has been done on the user trust in OSN. However, the essence of trust was added without considering the opinion of the user. It was observed that [11] among the users that were surveyed, many users are not much concerned about whom they are adding as friends. This is the reason why the data is leaked amongst the friends who are not intended to view that data. This leads to data confidentiality attack. The main idea behind the work is to add the flavour of trust in OSNs which depends on the system generated observations as well as the user's experience about that particular person.

Table 1 Comparison of related work [16]

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 [7]	Clustering methods, user generated ratings	No	Yes	No
New Algorithm for Trust Inference in Social Networks [12]	Probabilistic models	No	No	No
Experimental Analysis on Access Control Using Trust Parameter for Social Network [6]	Interactions between users and friends	Yes	No	No
Propagation Models for Trust and Distrust in Social Networks [8]	Propagation models	No	No	No
Finding the Optimal Social Trust Path [13]	Heuristic algorithms	No	No	No
Multiparty Access Control for Online Social Model and Mechanisms [5]	Trust is not considered	No	No	No
Operators for Propagating Trust and their Evaluation in Social Networks [14]	Trust metrics	No	No	No
Trust based approach for protecting user data in social networks [9]	Hop based technique	Yes	No	No
Proposed Scheme	Using experience, Context Information and Interaction	Yes	Yes	Yes

5.1 Calculating Trust Score

To calculate the trust in OSN following attributes are considered:

5.1.1 Experience (EX)

Experience is the user's experience with a particular person in the real life. A person tends to accept the friend request on the social networking site but may not have good experience with him in the real life. This is not system generated but is considered as the input to the system by the user. The experience means knowing that person in real life. It was observed that [3] among the surveyed people, about 82% add only those friends who they know in real life. However, knowing a person and trusting the person are two different terms. Hence, experience plays a vital role in determining the trust amongst the owner and his friends. The system motivates the user to classify the friends in his friend list into following three categories which can be defined as follows:

5.1.1.1 *Close friends*

People who are best known and who meet frequently and have good knowledge about each other's reactions come under this category. These are the highly trusted people with whom the person can share secured data. This feeling of trust is generated from daily interactions. For example, colleagues, best friends, relatives, family members, neighbours etc. However, whom to choose into this category is solely the user's choice as the definition of 'close friends' varies from person to person.

5.1.1.2 *Friends*

These are the general friends who are not much in contact. Also, the experience with them may be average or good but not too strong to give them the access of the secured data. These are the friends that have met in the real life but not so much that they were able to build a very good trust to share the secured data. For example, the new relations that were recently built up, colleagues belonging to same institution or company met only a few times.

5.1.1.3 *Less known*

These include the friends that are known but may not have very good relations with the person. Also the person may have very good past experiences with that particular person but that may not be the same with the present time. For example, the school going friend who has met you after long time, friend of friend, person with whom very less real life experiences are shared etc. Depending on the opinion chosen by the user, the crisp values are denoted for every fuzzy value.

Table 2 Values for EX

Fuzzy Value	Crisp Value
Close Friends	1
Friends	0.75
Less known	0.25

5.1.2 Context information (CI)

This mainly includes the two sub attributes that is, number of friends the person has and the dynamicity the person has on the OSN. Dynamicity refers to how much active the user is on the OSN. The dynamicity includes the number of posts, comments, frequency of change in profile etc. According to [3] all these factors are taken into consideration by the users while they accept the friend request. Here, we consider a factor which tells the deviation factor for number of friends which is calculated as follows:

$$\alpha = \frac{nof - 130}{nof} \tag{1}$$

Where nof is number of friends and 130 is the average friends [3] the user has according to the survey done. Thus lesser the value of α less are the number of friends. Now to calculate the dynamicity of the user, we consider how much active the user is considering the number of posts, comments, number of photos uploaded etc and compare this count with the number of times he logged in. let m be the value of any activity by the user like number of posts, comments photos uploaded etc and let n be the number of times the user has logged in. Dynamicity (D) is calculated as follows:

$$D = \frac{n}{m} \tag{2}$$

Thus lesser the value of D more dynamic the user is. The fuzzy values for D are identified as follows:

Table 3 Fuzzy rules for dynamicity

Case	Fuzzy Value
D >= 0.75	Less Active
0.75 > D >= 0.5	Average Active
D < 0.5	Highly Active

Now CI can be collectively calculated as follows using the fuzzy rules.

Table 4 Fuzzy rules to evaluate CI

D	nof	CI	Fuzzy Value For CI
Less Active	<0.5	0.5	Inactive
Average Active	<0.5	1	Active
Highly Active	<0.5	1	Active
Less Active	>0.5	0.5	Inactive
Average Active	>0.5	1	Active
Highly Active	>0.5	1	Active

5.1.3 Interaction (I)

The concept of interaction is studied from [6] which is one of the aspect that is used to calculate trust. But as mentioned earlier it is not the only aspect. Interaction as mentioned in [6] is the message, likes or comments between the users. However, interaction is limited to the messages exchanged between the users. The interaction is calculated in the same way as referred in [6]. From the interaction, credibility is counted [6]. The credibility has following membership values as mentioned in [6]:

Table 5 Membership values to evaluate interaction

Credibility Value (Cr)	Membership Function Value	Fuzzy Value
Cr >= 70	1	Frequent
70 > Cr > 50	0.5	Infrequent
Otherwise	0	None

Hence, the above factors can be used to derive the Trust score between the owner of the profile and all his friends in the friend list. According to [3], the survey of 1895 users was performed and they have noted the factors that people consider while they accept the friend request. Accepting the friend request is one of the action that a user does if he trusts the person. This is the ideal situation. From [3] the above factors that is, EX, I and CI was given some weights. These weights were calculated based on the percentages that were derived for each factor from the survey. The final weighted equation for the calculating Trust score required to calculate the weights of each factor (EX, CI and I). Hence, following formula was used:

$$w = \frac{Impact\ Factor}{Total\ Impact} \tag{3}$$

Here, Impact factor denotes the importance the people have given for each factor, that is, EX, CI, and I. For example as mentioned in [3], the EX is given

82% which is the highest importance given by the people when they accept the friend request. Hence,

$$\text{Impact Factor (EX)} = 0.82 \tag{4}$$

In the same way Impact factor is calculated for CI and I based on the real life survey in [3].

$$Total\ Impact = \sum Impact\ Factors\,(EX, CI, I) \tag{5}$$

Based on these calculations the final Trust equation was derived. The trust equation is defined as the weighted equation where weights are derived from Equation 3. Thus, the Trust score between the owner O with the friend $\mathrm{F_i}$ is defined as:

$$\mathrm{T_{O->Fi} = 0.614EX + 0.277CI + 0.109I} \tag{6}$$

Here the variable $\mathrm{T_{O->Fi}}$ denotes the trust score from owner O to friend $\mathrm{F_i}$. Hence, if there are n friends in the friend list of the owner O there are n trust values as shown below. Consider a set T of trust scores calculated from Equation 6. Hence, T is denoted as follows for all the n friends in the friend list of O.

$$\mathrm{T = \{T_{O->F1}, T_{O->F2, \ldots\ldots\ldots\ldots} T_{O->Fn}\}} \tag{7}$$

Thus, this matches with the concept real life trust. In the real life, every person has different level of trust on the other person. This means that the trust factor changes from person to person. Hence, Equation 6 also depicts the same concept. Following cases and possible values are derived for the Trust score taking into consideration all the combinations of values of EX, CI and I. These values are derived taking into consideration all the crisp values.

From the Table 6 it is observed that minimum trust can never be 0 as even though stranger is added he will always have some or little activity on OSN. This however is the ideal case. Figure 2 shows pictorially how the trust score is calculated. Also the Figure 2 depicts how the trust score calculation is dependent on the system process and user's opinion as well. The maximum trust is 1 when owner has highest trust in the friend $\mathrm{F_i}$ and $\mathrm{F_i}$ is active on the OSN and has frequent interactions with owner. It is observed that as the majority of the users give highest importance to the real life experiences with their friends, hence, the weight for EX is highest and highly affects the trust score. From the Table 6 it is seen that even if there are no interactions with

Table 6 Trust score values

Case	EX	CI	I	Trust Score (T)
1	Close Friend	Active	Infrequent	0.943
2	Close Friend	Active	Frequent	1
3	Close Friend	Active	None	0.891
4	Friend	Active	Infrequent	0.636
5	Friend	Active	Frequent	0.688
6	Friend	Active	None	0.584
7	Less Known	Active	Infrequent	0.482
8	Less Known	Active	Frequent	0.534
9	Less Known	Active	None	0.430
10	Close Friend	Inactive	Infrequent	0.804
11	Close Friend	Inactive	Frequent	0.856
12	Close Friend	Inactive	None	0.752
13	Friend	Inactive	Infrequent	0.497
14	Friend	Inactive	Frequent	0.549
15	Friend	Inactive	None	0.445
16	Less Known	Inactive	Infrequent	0.344
17	Less Known	Inactive	Frequent	0.396
18	Less Known	Inactive	None	0.292

the best friend of owner on the OSN like Facebook and even if the friend is not active (case 12) also owns a trust 0.752. The graph in Figure 3 shows how the trust score varies with the varying values of EX, I and CI. All the 18 cases from the table are represented in the above graph. From the Figure 3 it is observed that all the values range between 0 and 1. All the trust scenarios are considered in the graph. Also, the minimum trust in the worst case is 0.292. This is the trust score when the owner doesn't have good experience with the friend F_i, and F_i is not active and there are no interactions between owner and F_i. Though it is less than many cases shown in Figure 3, but is high enough to share secured data. Hence, even if the friend is less active and has not interacted with the owner does not mean that he is not trusted at all. Hence, the user input that is EX carries more weight to calculate the trust score so that owner's best and trusted friends in any case should not be deprived of valuable information from the owner. Also, the graph shows variation of Trust score with the other varying parameters like I, CI and EX. The trust score varies according to the weighted equation that is the trust score varies linearly with the variables that is, the attributes like EX, CI and I. Thus trust score has linear variation with all the attributes used to calculate the trust score.

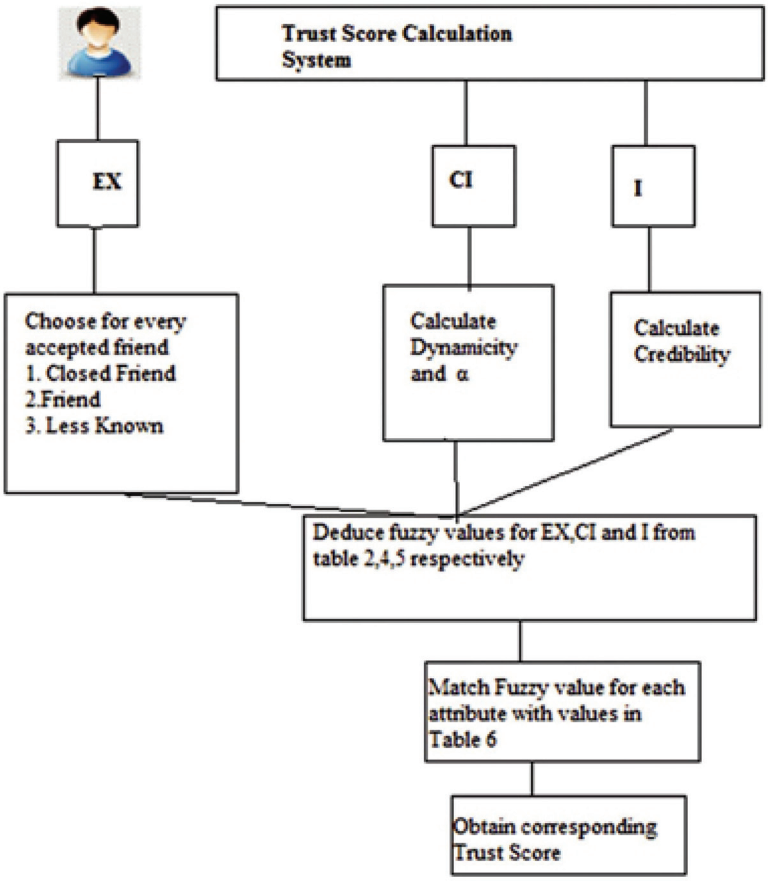
Trust Score Calculation System
EX
CI
I
Choose for every accepted friend
1. Closed Friend
2.Friend
3. Less Known
Calculate Dynamicity and α
Calculate Credibility
Deduce fuzzy values for EX,CI and I from table 2,4,5 respectively
Match Fuzzy value for each attribute with values in Table 6
Obtain corresponding Trust Score

Figure 2 Flow of trust score calculation.

5.2 Trust Rule

Trust score was mainly calculated to achieve access control to the confidential or secured data over OSN. Trust Rule defines the method by which this access control can be achieved. For every data that is uploaded by the user, he has to mention the security level. Hence, with every data that is uploaded by the owner a security level [5] is attached to it. For example if Alice uploads the photo of nature's scene from the hill station that she has visited recently, that will have very less security level. Instead if she uploads the photos of her with her friends and wants that only close friends should view it, she would assign high security level to it. This security level is the input from Alice as

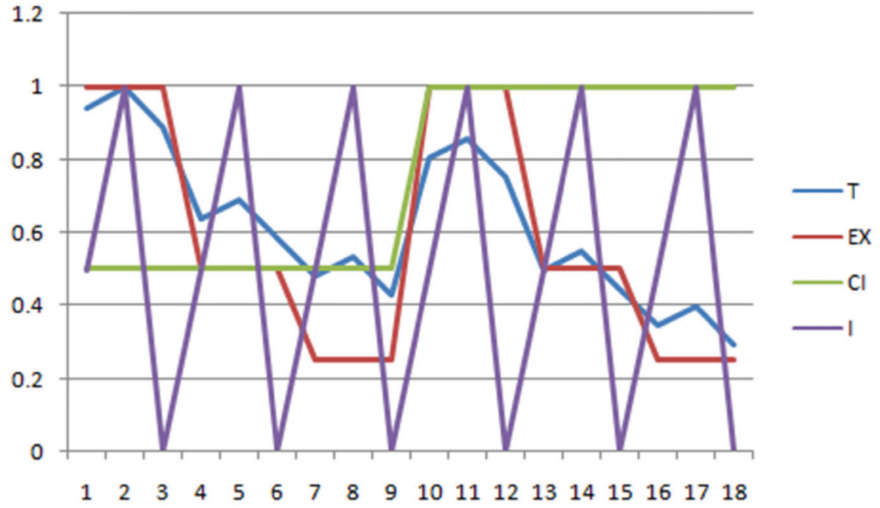

Figure 3 Graph representing the variations of trust score with variations in EX, CI and I (T).

she uploads the data. This security level is also called as trust threshold (T_{TH}). This is because:

$$Security\ Level\ \propto Trust\ Score \tag{8}$$

Higher the secured data, owner wants it to be seen by only the highly trusted users. Thus the security level that is given by the owner is same as the threshold trust score (T_{TH}). Now the Trust Rule is defined as follows:

Table 7 Trust rule

Case	Access Decision
$T_{O->Fi} < T_{TH}$	Access Denied
$T_{O->Fi} >= T_{TH}$	Access Allowed

$T_{O->Fi}$ is the Trust score between owner O and friend F_i. Thus Trust Rule controls the access to the data uploaded by the user and hence, is used in access control mechanism. According to the Trust Rule, only the users that are trusted by the owner are given access to the secured data while others are denied the access.

5.3 Trust Score System

As shown in the Figure 4, there are four main components that play important roles in trust score calculation and access control.

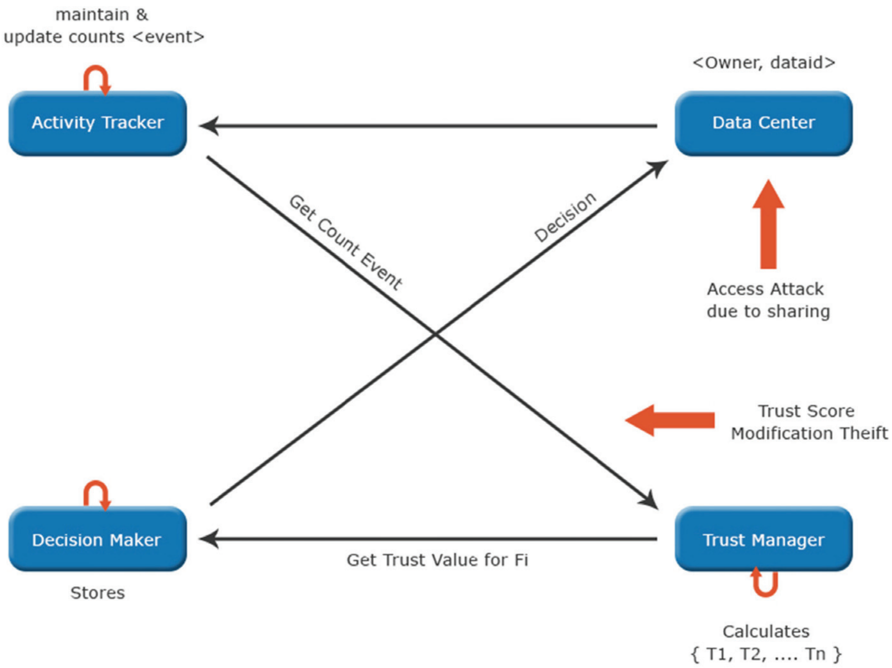

Figure 4 Trust score system.

5.3.1 Activity tracker (AT)

This component maintains and updates the required counts. For example, to calculate the dynamicity of friend of the owner, it is required to know the total number of posts and comments by the user, number of times he logged in, number of times the friend changed his profile like status, profile picture etc. All these counts are considered as the activity from the user. This activity is tracked by the Activity Tracker. The Activity Tracker stores or maintains these counts of every user along with user id. Also frequent modifications of the counts are also required. The counts are updated with the events that AT receives whenever, the user comments, posts or changes his profile details.

5.3.2 Trust manager (TM)

The main task of TM is to calculate the trust score for all n friends of the owner O. TM always receives the event from AT whenever it updates any count. With the event received from AT, TM again recalculates the trust score with the changed or updated counts and stores it in the form of $<T_{O->Fi}, O, F_i>$

Where,

$T_{O->Fi}$ is the trust score of friend F_i by the owner O.

O is the owner identified by the id

F_i is the friend id from O's friend list.

Also it recalculates the trust score if O changes EX value for F_i due to change in the real life experiences. Thus TM manages the most important job of trust score calculation. Hence, TM calculates

$$<T_{O->F1}, T_{O->F2,.....}T_{O->Fn}> \text{ for all n friends in the friendlist of O.}$$

5.3.3 Decision maker (DM)

Decision Maker is the component in the system which is responsible for the access control of the secured data. It stores all the values in the form of $<d, T_{TH}, O>$

Where,

d is the data uploaded by the owner O

T_{TH} is the security level or the threshold trust score

O is the owner.

DM takes the decision to allow or deny the access using T_{TH}, trust score from the TM and Trust Rule that was defined earlier. Thus it provides effective access control mechanism.

5.3.4 Data centre

Data centre stores all the data that is uploaded by the users of OSN. The data is stored in the 2-tuple format $<O, d>$.

Where,

O is the owner who uploads the data

d is the data id uploaded by the user

Whenever, data is uploaded on the OSN by the user, it is stored in the Data centre and its data id is generated and sent to DM along with owner id O. Data centre can be chosen to be put on the cloud. If the owner wants to change the security level of the data, it can be changed at the DM as it takes the decision regarding the decision to allow or deny access.

All the components of the system communicate with each other in the give and take of the data that is required by every component to finally achieve trust based access control.

As shown in Figure 4, two threats have been defined. Dealing with those threats is a future work.

5.4 Flow of Actions from User Perspective

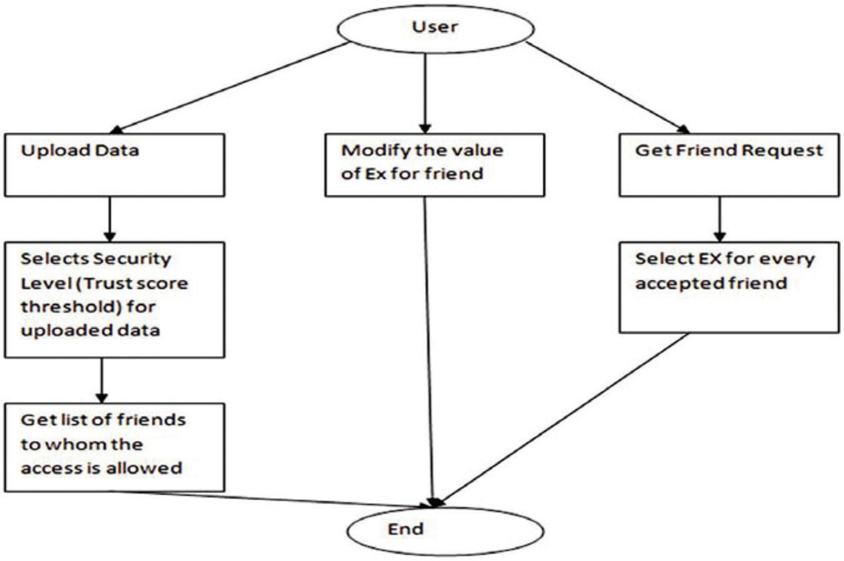
User
Upload Data
Modify the value of Ex for friend
Get Friend Request
Selects Security Level (Trust score threshold) for uploaded data
Select EX for every accepted friend
Get list of friends to whom the access is allowed
End

Figure 5 User flow of actions.

Figure 5 depicts the various tasks that the user performs while using the system. He uploads the data, adds the trust score threshold on which the Trust Rule gets implemented to provide the access control. Also he can view the friends to whom the access is given. With the change in the real life experience, the trust of owner towards a particular friend may increase or decrease. To absorb this real life fact in the OSN, the user can change the EX towards any of his friend. Whenever a user gets friend request he must allocate the EX to the friend. The system can be implemented using APIs as defined in [1].

6 Conclusion and Future Work

Trust plays an important role during interaction with the people in our daily life. As the people around the world are becoming more and more active on OSNs like Facebook, Twitter etc. adding the flavor of trust in OSN has also become the need of the time. Hence, an access control mechanism that works on the concept of trust was thought to be of greater importance. The proposed system calculates trust considering EX, CI and I as the three main attributes that helps in calculating the trust. Also, out of these three, CI and I are derived by the system and EX is the input from the user. The user attaches the security level with each data (photo, status, video) that she uploads. As the security level is same as available the threshold trust score, the decision is made to allow the access or deny the access depending upon the defined Trust Rule which contains the comparison between the trust score of every friend in the friend list and the threshold trust score given as the input from the user. The decision is generated by applying the Trust Rule which helps in access control of the information that is uploaded by the owner. Hence, the system achieves trust based access control using the system and user's decision which can be considered as the best and effective mechanism to calculate trust.

The threats have been identified in the system. However, to propose an effective solution against the threats is the future work. Voting mechanism can be used to handle the data confidentiality attack due to sharing of data. Also to design the algorithm for the system implementation is another future work. The system can be implemented using various APIs. (Graph API n.d.)

References

[1] Graph API available from <https://developers.facebook.com/docs/graph-api>

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

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

[4] https://www.stonetemple.com/how-are-people-using-facebook/

[5] Hongxin Hu, 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

[6] Saumya Omanakuttan and Madhumita Chatterjee, 'Experimental Analysis on Access Control Using Trust Parameter for Social Network', Springer-Verlag Berlin Heidelberg 2014

[7] Wei-Lun Chang & Arleen N. Diaz & Patrick C. K. Hung, 'Estimating trust value: A social network perspective', Springer Science + Business Media New York 2014

[8] 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

[9] 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

[10] Chi Zhang and Jinyuan Sun, University of Florida, Xiaoyan Zhu, Xidian University Yuguang Fang, University of Florida and Xidian University. 'Privacy and Security for Online Social Networks: Challenges and Opportunities', Network, IEEE Volume: 24, Issue: 4 DOI:10.1109/MNET.2010.5510913 Publication Year: 2010

[11] Hootan Rashtian, Yazan Boshmaf, Pooya Jaferian, Konstantin Beznosov, 'To Befriend Or Not? A Model of Friend Request Acceptance on Facebook', Symposium on Usable Privacy and Security (SOUPS) 2014, July 9–11, 2014, Menlo Park, CA.

[12] Ugur Kuter, 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)

[13] 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

[14] 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

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

Biographies

V. K. Takalkar graduated in Computer Science and Engineering from Pune University, Maharashtra, India in the year 2013. She has completed her Masters from Savitribai Phule Pune University. Her research interests are online network security and Internet of Things. She has published more than 6 papers in international journal and conferences. She has a teaching experience of 2 years. She is currently working as Assistant Professor in Department of Computer Engineering at Smt. Kashibai Navale College of Engineering.

P. 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 undergraduate students and 10 plus post-graduate students for projects. His research interests are Algorithms, IoT, Identity Management and Security.