Computers, Materials & Continua CMC, vol.62, no.3, pp.1143-1159, 2020

Access Control Policy Based on Friend Circle

Qin Liu[1], Tinghuai Ma[1, 2, *], Fan Xing[1], Yuan Tian[3], Abdullah Al-Dhelaan[3] and Mohammed Al-Dhelaan[3]

Abstract: Nowadays, the scale of the user's personal social network (personal network, a network of the user and their friends, where the user we call "center user") is becoming larger and more complex. It is difficult to find a suitable way to manage them automatically. In order to solve this problem, we propose an access control model for social network to protect the privacy of the central users, which achieves the access control accurately and automatically. Based on the hybrid friend circle detection algorithm, we consider the aspects of direct judgment, indirect trust judgment and malicious users, a set of multi-angle control method which could be adapted to the social network environment is proposed. Finally, we propose the solution to the possible conflict of rights in the right control, and assign the rights reasonably in the case of guaranteeing the privacy of the users.

Keywords: Social network, privacy protection, circle of friends, access control.

1 Introduction

Through the diverse services provided by social network sites, people can easily upload the various resources they own to the platform so as to share information with others. In addition, in order to make the management of enterprises more convenient and contact with partners closer, more and more enterprises have started to manage or contact with other enterprises using social network services. As the number of users owned by each social network site grows rapidly, there are a large number of user-related privacy data, such as personal identification, confidential documents and contact record with others. If these private data are not properly protected, they will be stolen or inadvertently leaked by others, which will bring serious harm to the users not only in the online society but also in the real world. Social network services can make users communicate and share information with each other [Rong, Ma, Tang et al. (2018)]. With the development and improvement of social network services, users can achieve more things they want to do on the platforms, such as uploading photos, evaluating things around them and so on. Therefore, users can make new friends and communicate with friends on social network

[1] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, 210044, China.

[2] CICAEET, Jiangsu Engineering Centre of Network Monitoring, Nanjing University of Information Science and Technology, Nanjing, 210044, China.

[3] Computer Science Department, College of Computer and Information Sciences, King Saud University, Riyadh, 11362, Saudi Arabia.

[*] Corresponding Author: Tinghuai Ma. Email: thma@nuist.edu.cn.

apps such as Facebook. Users put a lot of personal data on social network apps. For example, Facebook has more than 1 billion registered users' basic information, including name, age, education experience and so on. There are more than 3 billion new personal data generated every day Facebook fact sheet and statistics [Ma, Zhang, Cao et al. (2015)]. While enjoying the conveniences brought by social networks, users also worries about the security of their privacy data such as some personal information. Only providing a safe and reliable privacy protection, can users use various social network services with confidence. And thus social networks and various platforms and technologies related to it can develop better.

2 Related work

Nowadays, more and more researchers begin to pay attention to the research of privacy protection in social networks [Ma, Wang, Tang et al. (2016)]. What's more, the matching software industry standards have been formulated and the related technical frameworks have been realized.

(1) P3P privacy preferences platform

The P3P privacy preference platform [Reay, Dick and Miller (2009)] can provide a standard, machine-readable, and extensive format for privacy policies by protocol. It uses Web browsers to read privacy policies automatically and deal with it by judging the results. In this way, the ultimate goal of privacy protection is achieved.

(2) XACML

OASIS implements an access control markup language, which is XACML [Hong, He, Ge et al. (2017)]. The role of this kind of access control markup language is mainly two which includes describing the relevant content in the access control policy and implementing the access control decision. An important component of XACML is its root element, which is the Policy element. The root element of XACML [Ammar, Malik, Bertino et al. (2015)] is mainly composed of access control rules, and the access control rules are composed of condition elements and rule utility elements where the value of the rule utility elements is allowed or blocked. The value of the rule utility element is determined by the condition element. The value is allowed if the result of the condition element judgment is true. Otherwise, the value is deterred if the result of the condition element judgment is False.

(3) RBAC

Role-Based Access Control (RBAC) [Chakraborty and Ray (2016)] is widely used in rights management and privacy protection. The Role is an intermediary between user and privilege (a role can be seen as a group with multiple users, and these users have the same operations and the scope of responsibilities), which replaces the direct relationship between the original user and the privileges.

At present, researchers have proposed some corresponding solutions for privacy protection issues in social networks, but there are still many shortcomings. We mainly design authority allocation algorithms under the framework of RBAC, which makes it more reliable to assign access level.

3 Friend circle detection

Because our proposed access control algorithm is related to the circle of friends discovery algorithm [Ma, Rong, Ying et al. (2016); Lv, Ma, Tang et al. (2016)], we briefly introduce the related friend circle detection algorithm in this section.

3.1 Basic definition

The ego network is represented by an undirected graph $G(V, E)$, where V represent a set of nodes, that is, the set of users in the social network, $|V| = n$ is the number of nodes, $E \in V \times V$represents the set of edges which reflect the relationship between users and $|E| = m$ is the number of edges.

1. User attribute set

For each node v_i in V, we define its attributes as a collection $Attr_{v_i} = \{A_1, A_2, A_3, \dots, A_p\}$, where $A_j (1 \le j \le p)$ represents an attribute element.

It is important to note that some elements possess a single attribute value, and some elements can be divided into multiple attribute values $A_j = \{a_1, a_2, a_3, \dots, a_{jp}\}$, where jp represents the number of sub-attributes that A_j possess.

2. Central user

For the owner of the ego network, we define it as the central user which is represented by Cu and $Cu \in V$.

3. Friend set

For each node in V except for Cu, we define a friend set F = $\{f_1, f_2, f_3, \dots, f_{n-1}\}$, where $f_k (1 \le k \le n-1)$ represents a friend of the central user.

4. Central user attribute matrix

The attribute matrix of the central user $Vector_{Cu} = \left[Value_{A_1}, Value_{A_2}, Value_{A_3}, \dots, Value_{A_p}\right]$ is formed by attributes in the central user's attribute set $Attr_{Cu}$, .

5. Friend set attribute matrix

All of the attributes in $Attr_F$ form the attribute matrix of the friend set together, as shown below.

$$\begin{matrix} f_1 \\ \\ \\ \\ f_{n-1} \end{matrix} \begin{bmatrix} Value_{A_1} & Value_{A_2} & Value_{A_3} & \cdots & \cdots & Value_{A_p} \\ Value_{A_1} & Value_{A_2} & Value_{A_3} & \cdots & \cdots & Value_{A_p} \\ Value_{A_1} & Value_{A_2} & Value_{A_3} & \cdots & \cdots & Value_{A_p} \\ \vdots & & & & & \\ \vdots & & & & & \\ Value_{A_1} & Value_{A_2} & Value_{A_3} & \cdots & \cdots & Value_{A_p} \end{bmatrix}$$

3.2 Algorithm procedure

In this section, we introduce our circle of friends discovery algorithm in detail. First, we compare the similarities between central user and friend attributes. According to different

ways, including a single attribute comparison and multi-value attribute comparison, we will divide all friends based on attribute similarities. Then, for some friends whose attributes may not be complete or missing, we use the structural features of ego networks to further classify them. Whether a node representing a single friend should be added to a circle of friends is determined by two aspects: the probability that a node should be added to a circle of friends and how the value of the node changes after joining a circle of friends. Finally, we analyze the frequency of contact between the central user and his friends, which reflects the interaction between them. We use this value to find out some people who are in constant contact with the central user and put them into a specific circle of friends.

3.2.1 Attribute similarity

For each user in the social network, there are various attributes such as name, occupation, educational experience, hobbies, etc., as shown in Fig. 1. The relationship between a central user and his or her friend may depend on the similarity between the different attributes. For example, co-worker relationship requires people to have the same job, but the relationship of old boy require existing a same school in their educational experience. In order to truly distinguish all the different relationships between the central users and their friends, we divide circle of friends according to different attributes. That is, some friends in the same circle of friends is because of the same occupation. But for another circle of friends, this is because of similarities in educational experiences. In this respect, some of your friends are scheduled to be part of their circle of friends because they have the same attributes as their center users. In addition, it is noteworthy that a user may be arranged in more than one circle of friends because he has not only one common attribute with the central of the user.

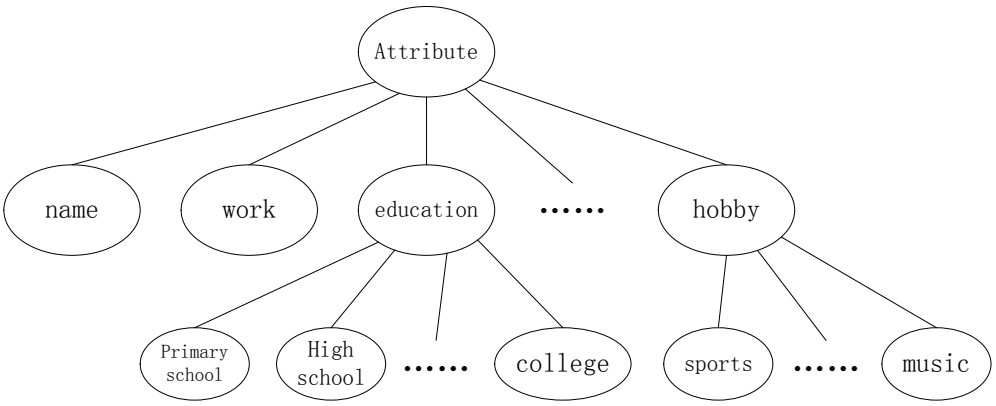


Figure 1: User attribute map

When the number of attributes is huge, especially when the number of user data is less than the number of attributes, it can lead to problems. On the one hand, high attribute dimension will consume lots of time even if there is only a small amount of user data, which makes the algorithm perform bad. On the other hand, the importance of each attribute is not the same. Therefore, we need to conduct the attribute selection process first, so as to select the attributes that can provide important information called the main attributes. Through this process, we can achieve the purpose of reducing the attribute

dimension. After the attributes are selected, we will identify the relationship between the central user and his or her friends by comparing these selected attributes.

For each main attribute, as long as a friend has similar attributes to the central user, the friend is added to the circle of friends related to the main attribute. For the other attributes (not main attributes), we define a threshold as the minimum similarity value to determine whether to add a friend to the circle of friends named buddy based on attribute similarity.

3.2.2 Contact frequency based similarity

As we know, the relationship between people is not static over time. A person may have good relationship with someone during this time, but at another time they connect more frequent with other people. We tend to tell the private information to them who we connect more frequent and have a good relationship with us at recent time. Therefore, we introduce a parameter named contact frequency that considers this characteristic to make the result more reasonable and dynamic. Through this parameter, we can observe the recent contacts between two people.

In social network services, users can communicate with each other via private messages, comments, repost and so on. In the designated period of time, the more contacts two people have, the higher frequent contact that two people have. The higher frequency of contact means that the better the relationship between two people.

In summary, our algorithm mainly consists of the following two parts:

(1) First, we choose the main attribute according to the information gain. Assigning friends to different circle of friends by comparing the values of attributes that central users and friends have.

(2) Finally, we calculate the contact frequency between friends and the central user, which reflects the frequency of recent contact between the central user and his friends, so as to find out a few friends with the highest contact frequency and add them to a new circle of friends, which is frequent contact circle of friends.

4 Access control algorithm in personal network

In this section, we first divide the information sensitivity and find out the personal information that affect users in various degree. Based on this, a set of three levels of privacy access is proposed. Then, on the basis of the circle of friends obtained in the previous section, we consider the aspects of direct judgment, indirect trust judgment and malicious users, a set of access control method which could be adapted to the social network environment is proposed. We can give friends who are intuitively close to the central users a higher level of privacy access and at the same time we can use the judgment process of the malicious users to reduce the possibility of adverse factors for central users.

4.1 Privacy of personal information

Privacy information is included in the scope of the user's personal information, but not all of the user's personal information is privacy. In recent years, we have heard more and more incidents that have occurred as a result of the disclosure of personal privacy

information. This kind of privacy information is called sensitive information. The disclosure of sensitive information often brings risks to users. Therefore, under the circumstance that a large amount of user's personal information is contained in the social network today, it is an inevitable trend to divide the privacy level of the user's personal information and perform effective protection actions. The level of privacy of a user's personal information is intended to indicate the extent to which the user is willing to disclose information to others.

4.1.1 Sensitivity of personal information

The sensitivity mentioned in this section refers to the importance of information, which is related to the concern degree of the center of the user.

Table 1: Sensitivity of personal information [Hui, Teo and Lee (2007)]

Personal Information	Average Sensitivity	Number of objects
Hobby	1.61	98
Gender	2.31	103
Marriage	2.51	99
Nationality	2.74	109
Degree of education	2.79	19
Work	3.04	77
Education	3.19	16
Family	3.60	70
Name	3.83	109
Email	3.87	109
Address	5.02	109
Salary	5.25	64
Phone number	5.79	84
ID number	5.81	62
Credit	5.92	24
Bank account	6.53	49

The range of personal information is wide, Greniner [Greiner (2003)] conducted a summary analysis of the previous research, and summarize that the consumer information related to commerce companies is roughly composed of three attributes: population overview, financial status and the communication information, where the sensitivity is different if the information does not belong to the same category. Researcher Hui et al. [Hui, Teo and Lee (2007)] studied the relevant information of Internet users and found that the user's ID number, deposit information and other confidential information are sensitive while some demographic characteristics, such as gender and marital status, are less sensitive. Phelps et al. [Phelps, Nowak and Ferrell (2000)] studied the degree of willingness that a consumer agree to provide to the website and found that information

about personality traits is more important than financial information. Chinese researchers Huang et al. [Huang and Xu (2005)] obtained the online consumption information of China, the United States and France and analyze the sensitivity of these research population to the privacy information. The results show that financial information is the most sensitive information for consumers. Although the definition of sensitive information is not exactly the same for everyone, in most situations, if the research population is consumer, they are more sensitive to medical and financial information than other information. In this paper, we use the statistical results obtained by Hui et al. on the sensitivity levels of various types of information.

4.1.2 Division of privacy access level

According to the information sensitivity Tab. 1 summarized in the previous section, we divide the sensitivity of information into three levels: low, medium and high. The sensitivity of information is low if the average sensitivity is below 3.00. The sensitivity of information is medium if the average sensitivity below 5.00. And if the average sensitivity is above 5.00, we consider the sensitivity of information is high. Among them, the low-sensitivity information indicates that even if the information is leaked, it will not affect the privacy protection of the central user. The medium-sensitivity information may already be able to accurately locate some contact information or educational experiences of the central user, but it is difficult to find the user in real world. However, the high-sensitivity information is related to the user's own address, contact information and financial which will cause great harm to central users if these information is obtained by unscrupulous people.

For the above reasons, we divide the privacy access level as follows:

1) Basic privacy access level. This level is the basic privacy access for all friends, a friend can view all the low-sensitivity information of central user.

2) Medium privacy level. This level is the privacy access for friends who the central user rather trusts. These friends can view both the user's low-sensitivity and medium-sensitivity information.

3) Higher privacy level. This level is the privacy access for friends who the central user trusts most. These friends can view both the user's all kind of sensitivity information.

4.2 Access control based on level of trust

Level of trust refers to the trustworthiness of a friend for the central user. In other word, it reveals that whether a central user is willing to disclose private information to a friend. A central user is willing to tell more about his or her personal privacy to a friend if the level of trust of this friend is higher. And at the same time, the level of privacy is higher.

Quantification of trust mainly depends on three aspects. First, the circle of friends which the friend is located in and the weight of the circle of friends. The second is the number of mutual friends between the central user and friend. The third one is the existence of malicious users.

4.2.1 Judgement based on circle of friends

We will disclose different personal information to different people according to the distance with them. The closer we are, the more we will disclose to them. At the same time, some people have a special relationship with us, such as colleagues or students. For such people, regardless of their relationship with us, they can know our occupation, educational experience, major and so on. Based on this feature, we will judge the different privacy levels of friends in this section based on the above two factors.

In the previous section, we divided friends into different circle of friends according to the attributes of friends of the central users, the distribution of friends in social networks, and the frequency of contact. Different circles of friends reflect the difference in the relationship between each friend and the central user and some friends who have special relationship with the central user. Therefore, we will make an intuitive judgment on the trustworthiness of friends based on the previous classification results.

We define the main attribute and the non-main attribute by feature selection. Friends with special relationships with the central users can be selected by circle of friends built according to the main attributes, such as the colleague circle divided by work and the classmates circle divided according to school. And the circle of friends divided according to non-main attributes is more dependent on the common interests or the common location. In the former case, no matter whether the relationship between the central user and these friends is close or not, the related attributes are always allowed to be gotten by each other. In the latter case, depending on the distance of relationship between the central user and his or her friend, different levels of privacy may be given to these friends. Circle of friends divided by the contact frequency can effectively provide us with a valid basis for the relationship between the central user and friends. It is also worth noting that each friend can be assigned to more than one circle of friends. For such friends, we will examine the level of trust that he meets respectively.

Based on the above ideas, in order to obtain more reliable result, we will follow the following process:

1) First, we will give them a basic level of privacy for all our friends. For all friends with this level of privacy, only low-sensitive personal information owned by the central user can be seen;

2) Then, for each friend, we will find out all the circle of friends he belongs to and calculate the level of trust he has;

3) Traversing all the circle of friends that a friend belongs to is the third step. If the friend belongs to one or more circles of friends related to main attributes, the friend can get the information of the central users in these circles besides the basic level of privacy;

For example, if a friend belongs to a colleague circle, he or she will be able to view the professional information of the central user besides the basic privacy level.

4) If the friend belongs to the buddy circle, he can still view the medium level of sensitive information owned by the central user besides the access rights that he already has;

5) Finally, a friend also belonging to the frequent contact circle indicates that the friend has been closer to the central user in recent time. Therefore, the friend can still view the more secretive personal information. For example, a friend may get the medium level of

sensitive information before, and now he or she can also get the high level of sensitive information;

6) The final privacy level is assigned to friends.

4.2.2 Judgment based on indirect level of trust

The level of trust obtained by the objective attributes of friends and central users belongs to a kind of direct evaluation criterion. In addition, sometimes although there is no relationship between two person or the relationship seems to be relatively distant, they can also achieve a rather trust relationship if they have many mutual friends. Therefore, based on the number of mutual friends between the central user and the friend, we can obtain the indirect trust level of the central user to a friend.

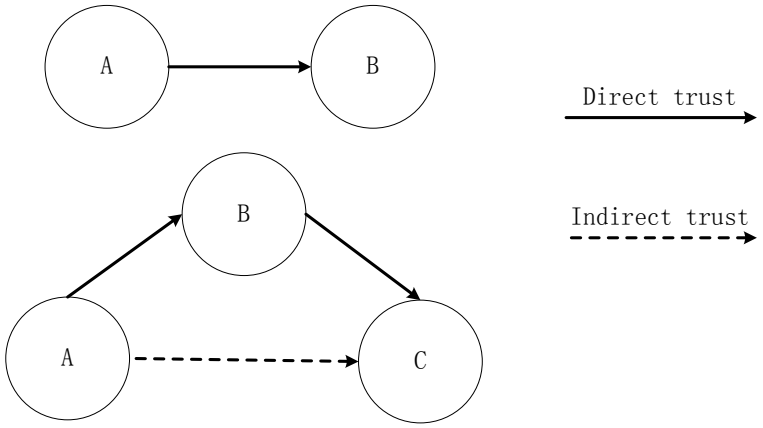


Figure 2: Direct trust relationship and indirect trust relationship

In this section, we will get an indirect level of trust based on the number of mutual friends between the central user and friends. After that, a set of level of privacy based on the number of mutual friends is obtained.

For the structural graph generated by the social network, when two nodes (denoted as point A and point B) are connected with the same node, it means that the node is a public neighbor of A and B. In social networks, the node represent the mutual friend between two people. Two node is closer if they have more common neighbors which are mutual friends. In order to find out trusted friends more accurately and protect the privacy of central users, we believe that friends who are greatly trusted by the central users are effective mutual friends.

As shown in Algorithm 1, during the preparation phase, the input data is the buddy circle that has been calculated in the previous section, and those nodes called candidate nodes that only have the basic privacy level. In the core part of the algorithm, it verifies whether these nodes meet the requests to obtain a higher level of privacy.

First of all, all the neighbor nodes of the candidate nodes are found. Then for each neighbor node of the candidate nodes, check whether it belongs to the buddy circle of central user. If so, we increase the number of the node's mutual friends with the central user by one. After traversing all the neighbors of this node, if the number of the mutual

friends between the node and the central user is greater than a certain threshold (such as 10), it is recorded as a node satisfying the condition and added to the satisfying condition set.

According to Algorithm 1, we can find out all the friends who have more than 10 mutual friends with the central user and only get basic level privacy. For those friends, we think they can get a higher level of privacy which is the medium level of privacy information. However, because these users are judged by indirect level of trust, they can't view the high level of sensitive information of the central user for security reasons.

Algorithm 1 Indirect trust judgment

Input: Center user's buddy circle; All candidate nodes

Output: Nodes satisfying condition (satisnode)

```
for node in all candidate nodes:
  find all neighbors of node
  for neighbor in all neighbors:
    if neighbor∈buddy:
      comfri++
    else:
     continue
    end if
  end for
 if comfri>10:
   satisnode=satisnode∪node
end for
return satisnode
```

4.2.3 Malicious users

In social networks, due to we cannot identify the user's identity, some users will do bad things thinking no one knows who they are, such as using uncivilized words to attack other users. For such users, social networking sites have basically launched the reporting function. Through this function, users who are excluded by other users because of some uncivilized behavior can be identified.

For malicious users who have been reported, we think this person has a potential risk factor for the central user. Therefore, for the purpose of protecting the security of central users, such friends are given the basic privacy right, that is, they can only see the low-sensitive personal information that the central user has.

4.2.4 Access conflict

Access conflict refers to conflicting permissions because the user has multiple roles or negligence of administrators. Encountered the case of access conflict, it cannot simply determine what kind of results should be implemented. Therefore, in order to make the

access control system run stably, it is necessary to consider the potential access conflict in advance and give corresponding solutions.

In this paper, the access conflict refers to that a friend may have three different privacy access level, because of the three judgement ways. How to solve this inconsistency and get the privacy right as accurately as possible in the case of privacy security protection of the central users is the problem to be solved in this section.

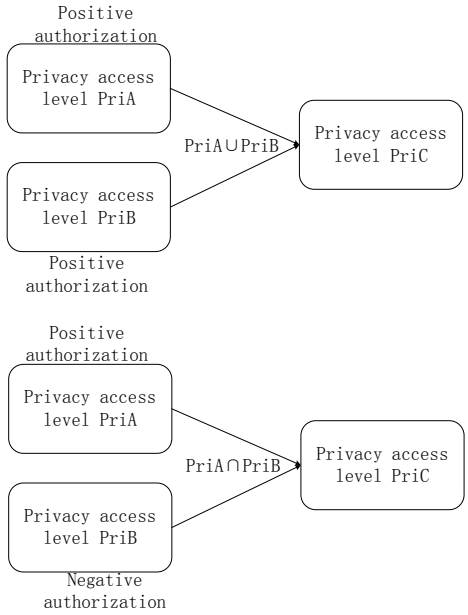


Figure 3: Resolution of access conflict

The main purpose of this paper is to protect the privacy of central users' personal information. Therefore, all the questions we mentioned is focus on protect the privacy. Therefore, a solution to the problem of access conflicts based on the security of central users' privacy information is proposed.

First of all, we consider that the privacy access can be divided into two types, one is positive access, which allows a friend to view the personal information, and the other is negative access, which does not allow friends to access personal information. The difference of positive authority means that the friend satisfies different conditions under different judgment conditions and thus one has a higher level of privacy access and another has a lower privacy access level. The difference of negative authority means that although a friend satisfies the condition of positive access but at the same time, he or she is given negative access for some reason. In our opinion, for the different types of positive access, we adopt the upward compatible strategy, which means the highest level of privacy, and for the different types of negative access, we use the downward compatibility strategy which means that we give the friend the lowest level of privacy.

The judgment method is as follows:

After judging based on circle of friends and indirect trust, if the results for the same friend is different which means the positive access is different, it represents that the

friend has satisfied the condition and can be trusted by the central user. And thus, we give this friend one of the two results with a higher level of privacy.

After performing judgment based on circle of friends, indirect trust level, and detection of malicious users, if the judgement for the same friend based on circle or level of indirect trust is different from the judgement based on detection of malicious users which means the negative access is different, it represents that the friend was given the level of privacy higher than the basic privacy level at the first two judgments, but later it was checked that the friend was a malicious user. In this case, we only give this friend the basic privacy level for the purpose of safeguarding the privacy of the central users.

5 Experiment

In this section, we will perform a simulation experiment on the access control method proposed in Section 4 to verify its validity. Because the accuracy of the permission setting is often determined by the user's subjective will, conflict resolution and dynamic permission set are two main objective factors of our experiment.

5.1 Experiment data

We use a personal web dataset crawled from three major social network sites: Facebook, Google+ and Twitter. All of these personal network data not only provides the personal information of all users but also the structural information of these social networks.

For Facebook, there are 10 personal networks, including 193 circle of friends and 4039 users. The data includes 26 user attributes, including birthdays, hometown, career and so on.

For Google+, there are 133 personal networks, including 479 circle of friends and 106,674 users. The data includes 6 user attributes, including last name, gender, job, university, organization, and place of residence.

For Twitter, there are 1000 personal networks, including 4869 circle of friends and 91,362 users. This data is collected from the Tweets and at used by each user.

These datasets do not contain the frequency of contact, so we collect the data through a questionnaire. 20 people are involved in our survey of frequent contact friends selection. Of the 20 participants, 10 are men and 10 are women. The participants consist of 17 students and 3 teachers, all of whom volunteered. Each of our participants have an average of 113 friends. The maximum number of friends is 302, the minimum is 41. During the investigation stage, each participant was asked to manually pick up 10 friends whom they thought should be added to frequent contact circles. In the end, there are 20 personal networks in total, including 147 circles of friends and 1154 users.

5.2 Conflict resolution verification

We select data with the contact frequency from the above data set to conduct experiments and randomly added a small number of malicious users to verify the reliability of the conflict resolution.

Table 2: Privacy privilege level in different situations

Friend type		Friend circle						Mutual friend	Privacy access level
		Classmate	colleague	Community member	Buddy	Frequent contact	Malicious user		
Contain main attributes	A	√						4	low+
	B			√				16	medium+
	C		√		√			12	medium+
	D			√		√		8	medium+
	E	√		√	√	√		22	high
Does not contain main attributes	F							3	low
	G							11	medium
	H				√			6	medium
	I					√		15	medium
	J				√	√		9	high
Malicious user	J	√				√	√	19	low
	K		√	√	√		√	3	low
	L				√	√	√	16	low

In Tab. 2, if friends belong to a variety of different circle of friends, we will select the representative of them. What's more, according to the access control scheme and conflict resolution strategy proposed in Section 4, different privacy permission controls are implemented.

Among them, the central user's friends are divided into three main categories: the friend whose friend circle contains the main attribute, the friend whose friend circle does not contain the main attribute and the friend who is the malicious user. For the first type of friend, when the user (friend) does not belong to the Buddy circle and does not belong to the frequent contact circle, the initial privacy access level of it is low+; when the user belongs to the Buddy circle or frequent contact circle, the initial privacy access level is medium+; when the user belongs to both the Buddy circle and the frequent contact circle, the initial privacy access level is high. Among them, low, medium and high access level represent that the friend can view the low-sensitivity personal information, medium-sensitivity personal information and high-sensitivity personal information of central user respectively. The "+" symbol indicates that the friend is also able to access the relevant main attribute corresponding to the main attribute circle which it belongs to. Since the high sensitivity information already contains all the main attribute information, there is no high+ privacy access level. In addition, when the number of mutual friends between the friend and the central user is greater than 10 and the initial privacy access level of the friend is low+, the privacy level of the friend is raised to medium+. For the second type of friend, because this type of friend does not belong to any of the main attribute circle of friends, so the privacy permission level is simple low, medium and high (i.e., does not exist "+"), the corresponding judgment method is basically similar to the first type. For the third type of friend who is a malicious user, regardless of which friends circle the

friend belongs to or how many common friends there are, the access level of he or she can only be low.

In summary, according to the access control and conflict resolution scheme proposed in Section 4, for a variety of different types of friends, correct access level can be assigned. What's more, it can solve the problem of conflicts. Therefore, it proves that the conflict resolution is effective and reliable.

5.3 Dynamic changes

When the circle of friends which a friend belongs to changes, the access level of this friend will change accordingly. In addition, when a new friend joins into the personal network of the central user, it will also need to assign corresponding privacy right to this new friend. In this subsection, we mainly verify the dynamic change function when the above situation occurs.

For a friend, there are five main types of changes that may occur:

(1) Joining Buddy or frequent contact friend circle;

(2) Dropping out of Buddy or frequent contact friend circle;

(3) Joining a main attribute friend circle

(4) Dropping out of a main attribute friend circle;

(5) Becoming a malicious user

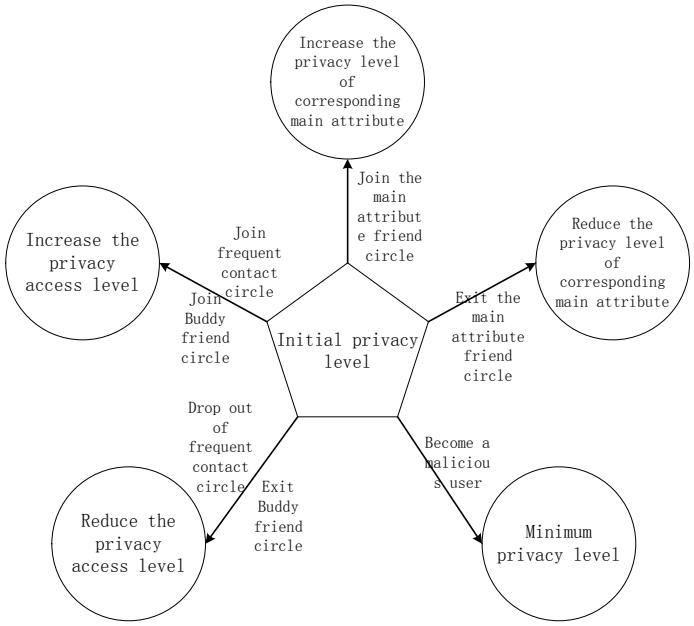
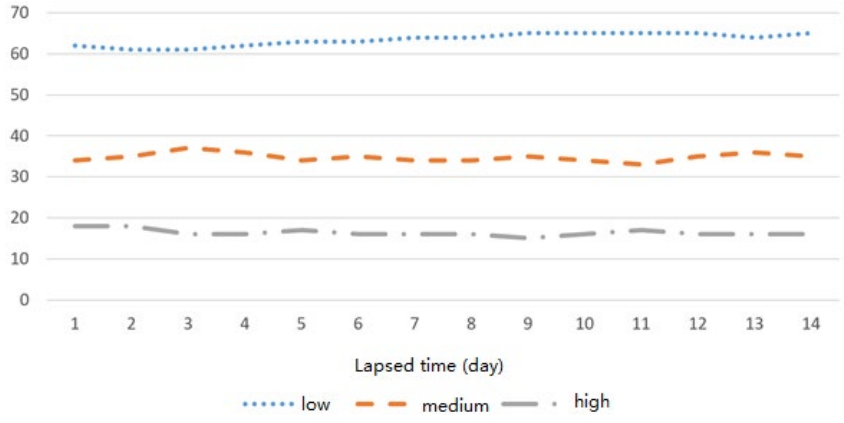


Figure 4: The change of privacy access level

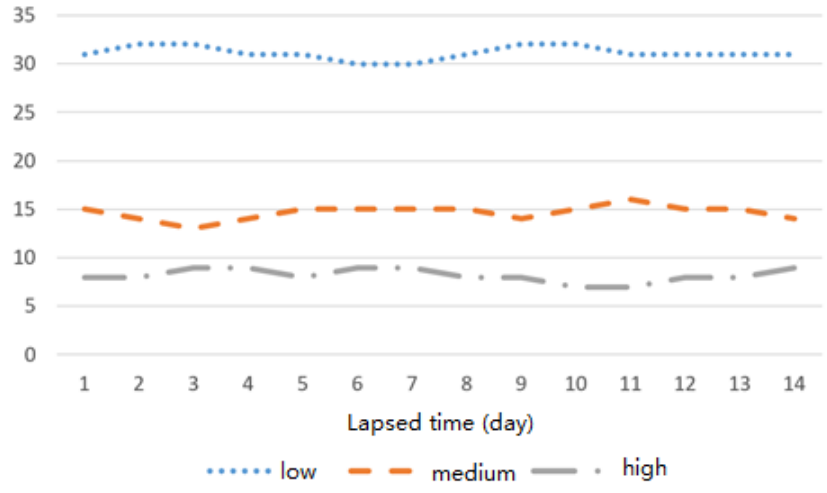
For the changes of five different circle of friends, Fig. 4 shows the changes in the corresponding privacy access level, including raising the access level, reducing the access level, increasing the access level of corresponding main attribute, reducing the access level of corresponding main attribute and directly becoming the lowest access level.

In addition, when the number of mutual friends between a friend and a central user changes, the corresponding change in the privacy permission level will also occur. That is, when the initial access level is low and the friend is a non-malicious user, the number of mutual friends is changed from 10 or less to 10 or more, the level of it is increased. When the initial level of privacy is medium and the number of friends is changed from 10 or more to 10 or less, if the friend does not belong to the Buddy circle and does not belong to the frequent contact circle, the access level of it will be reduced.

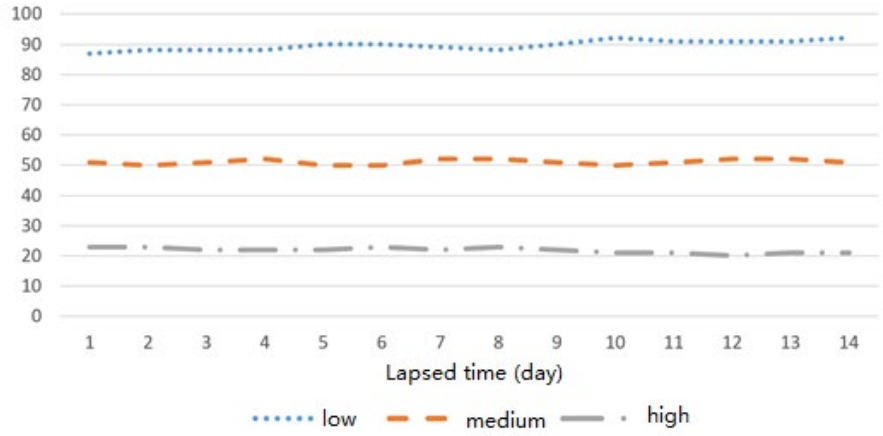
In order to verify the change of permissions in the real environment, we conducted a 14-day dynamic observation of the permissions of multiple groups of friends, and selected three sets of experimental results, as shown in Fig. 3. Among them, the main attribute circle of friends changes relatively little, so low + and medium + are not listed separately.



(a) Group 1



(b) Group 2



(c) Group 3

Figure 5: Dynamic change of permission

The low, medium and high in the Fig. 5 represent the total number of friends with low, medium and high access level respectively. It can be seen from Fig. 5 that as time changes, the total number of friends at each privacy privilege level does not change much. Through specific analysis, it is found that most of the changes are due to the update inside the frequent contact circle of friends. At the same time, although the changes shown in the Fig. 5 are not obvious, but in fact, when there is a friend's access level changed from one level to another level, there is another person has made the opposite change in most cases which resulting in a unobvious changes.

In summary, with the change of time, the access control scheme proposed can effectively realize the dynamic control of privacy rights, and can help the center users to implement the privacy protection function more flexibly.

6 Conclusion

In this paper, we propose an improved access control strategy to solve the privacy protection problem in personal networks, which is how to assign different access rights to different users according to various metrics. In details, based on the hybrid friend circle detection algorithm, we propose a set of flexible and accurate authority control schemes to adapt to the social network based on judgement of friend circle, judgment of indirect trust and malicious users. Finally, we conducted corresponding experiments and proved the superiority of our algorithm.

Acknowledgement: This work was supported in part by National Science Foundation of China (No. 61572259, No. U1736105). The authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through research group no. RGP-VPP-264.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

Reference

Ammar, N.; Malik, Z.; Bertino, E.; Rezgui, A. (2015): Xacml policy evaluation with dynamic context handling. *IEEE Transactions on Knowledge & Data Engineering*, vol. 27, no. 9, pp. 2575-2588.

Chakraborty, S.; Ray, I. (2016): Trustbac: integrating trust relationships into the RBAC model for access control in open systems. *Proceedings of the ACM Symposium on Access Control Models & Technologies.Lake Tahoe*, vol. 18, no. 37, pp. 49-58.

Greiner, L. (2003): Information requested is none of company's e-business. *Computing Canada*, vol. 29, no. 19, pp. 19-19.

Hui, K.; Teo, H.; Lee, S. (2007): The value of privacy assurance: an exploratory field experiment. *Mis Quarterly*, vol. 31, no. 1, pp. 19-33.

Huang, P.; Xu, H. (2005): The comparative analysis about information sensitivity among the consumers from China, USA, and France. *Systems Engineering-Theory Methodology Application*, vol. 14, no. 3, pp. 259-263.

Hong, R.; He, C.; Ge, Y.; Wang, M.; Wu, X. (2017): User vitality ranking and prediction in social networking services: a dynamic network perspective. *IEEE Transactions on Knowledge & Data Engineering*, vol. 29, no. 6, pp. 1343-1356.

Lv, Y.; Ma, T.; Tang, M.; Cao, J.; Tian, Y. et al. (2016): An efficient and scalable density-based clustering algorithm for datasets with complex structures. *Neurocomputing*, vol. 171, pp. 9-22.

Ma, T.; Rong, H.; Ying, C.; Tian, Y.; Al-Dhelaan, A. et al. (2016): Detect structural‐connected communities based on BSCHEF in c-dblp. *Concurrency & Computation: Practice & Experience*, vol. 28, no. 2, pp. 311-330.

Ma, T.; Wang, Y.; Tang, M.; Cao, J.; Tian, Y. et al. (2016): Led: a fast overlapping communities detection algorithm based on structural clustering. *Neurocomputing*, vol. 207, pp. 488-500.

Ma, T.; Zhang, Y.; Cao, J.; Shen, J.; Tang, M. et al. (2015): Kdvem: a k-degree anonymity with vertex and edge modification algorithm. *Computing*, vol. 70, no. 6, pp. 1336-1344.

Phelps, J.; Nowak, G.; Ferrell, E. (2000): Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, vol. 19, no. 1, pp. 27-41.

Rong, H.; Ma, T.; Tang, M.; Cao, J. (2018): A novel subgraph k+ -isomorphism method in social network based on graph similarity detection. *Soft Computing*, vol. 22, no. 8, pp. 2583-2601.

Reay, I.; Dick, S.; Miller, J. (2009): A large-scale empirical study of p3p privacy policies. *ACM Transactions on the Web*, vol. 3, no. 2, pp. 1-34.