A Random-Walk Based Privacy-Preserving Access Control for Online Social Networks

You-sheng Zhou
College of Computer Science and Technology,
Chongqing University of Posts and Telecommunications, Chongqing 400065, CHINA
School of Electronic Engineering,
Dublin City University,
Dublin 9, IRELAND

En-wei Peng
College of Computer Science and Technology,
Chongqing University of Posts and Telecommunications,
Chongqing 400065, CHINA

Cheng-qing Guo
National Computer Network Emergency Response
Technical Team/Coordination Center of China,
Beijing 100029, CHINA

***Abstract*—Online social networks are popularized with people to connect friends, share resources etc. Meanwhile, the online social networks always suffer the problem of privacy exposure. The existing methods to prevent exposure are to enforce access control provided by the social network providers or social network users. However, those enforcements are impractical since one of essential goal of social network application is to share updates freely and instantly. To better the security and availability in social network applications, a novel random walking based access control of social network is proposed in this paper. Unlike using explicit attribute based match in the existing schemes, the results from random walking are employed to securely compute L1 distance between two social network users in the presented scheme, which not only avoids the leakage of private attributes, but also enables each social network user to define access control policy independently. The experimental results show that the proposed scheme can facilitate the access control for online social network.**

Keywords*—online social networks; access control; random walk; privacy-preserving

I. INTRODUCTION

In recent years, the popularity of online social networks, such as Facebook and Twitter has grown tremendously. Users of social networks can easily establish relationships with people worldwide, and social network has become an indispensable communication platform in daily life. However, users usually obsessed with security risk when they shared pictures or news using on social network [1]. To address this problem, the traditional solution is employ attribute based access control. For example, when an online social network user A views his friend B's page, he notices a message posted by C, then he attempts to view C's page by clicking the links of B and the request of A will be sent to C. However, A is not a friend of C as shown in Fig. 1,the access control mechanism will be enforced before C making a decision on A's request. In the traditional attribute based access control scheme, A's attribute information will be requested to match the access control policy. As shown in Fig. 1, each online social network user should have multiple attributes a_i , which represent his social attributes, such as gender, age, email, contact, school etc. However, some attributes are sensible for the user, and the online social network user, such as A, is unwilling to reveal the attributes to others. Once the access control process is executed, C knows the attribute information of A. Undoubtedly; this attribute based access control method cannot prevent the user's privacy.

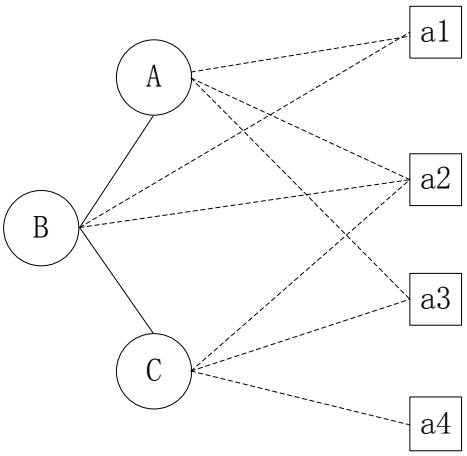

Fig. 1. Social-attribute Network

To address these privacy leaking problems, a novel random walker based access control for social network has been proposed in this paper. Unlike the classic access control schemes use attribute directly, our scheme utilizes the results of random walking as the inputs for distance protocol [2], which is used to evaluate the close relationship between two users. Furthermore, Paillier homomorphic encryption is integrated to our scheme to prevent the derivation of relationship using the results of random walking.

The rest of this paper is organized as follows: The related works are described in Section II. Section III focuses on preliminaries of truncated random walking and Paillier

homomorphic encryption. In Section IV, the concrete construction of the proposed access control is introduced. Implementation of our scheme and analysis are presented in Section V. Finally, the conclusion is made.

II. Related Work

Previous researches on access control for OSNs mainly focus on social graph structure, such as [3-5]. The D-FOAF system [3] is primarily of a friend ontology-based distributed identity management system for social networks, where access rights and trust delegation management are provided as additional services. In D-FOAF, relationships are associated with a trust level, which denotes the level of friendship existing between the users participating in a given relationship. Although the work discusses only generic relationships, corresponding to ones modeled by the FOAF: knows RDF property in the FOAF vocabulary [6], another D-FOAF-related paper [7] considers also the case of multiple relationship types. As far as access rights are concerned, they denoted authorized users in terms of the minimum trust level and maximum length of the paths connecting the requester to the resource owner. In work [4], authors adopt a multi-level security approach, where trust is the only parameter used to determine the security level of both users and resources. In the work [8], a semi-decentralized discretionary access control model and a related enforcement mechanism for controlled sharing of information in OSNs is presented. The model allows the specification of access rules for online resources, where authorized users are denoted in terms of the relationship type, depth, and trust level existing between nodes in the network. Barbara [9] has proposed an extensible, fine-grained OSN access control model based on semantic web technologies, and the main idea is to encode social network-related information by means of ontology. Those works all base on classical access control, they have ignored the process of classical access control may also leak users' social attributes. Fu [10] has proposed an attribute privacy preservation scheme based on node anatomy. It allocates original node's attribute links and social links to new nodes to improve original node's anonymity, thus protects user from sensitive attribute disclosure. Meanwhile, it measures social structure influence on attribute distribution, and splits attributes according to attributes' correlations.

Random walking algorithm is used for privacy preserving widely. Pili et al. [11] designed a protocol, which transforms community detection to a series of Private Set Intersection instances using Random walking algorithm. Gabor et al. [12] introduced a light-weight protocol to quickly and securely compute the sum of the inputs of a subset of participants assuming a semi-honest adversary. In this protocol, random walkers are performed over the network. Prateek et al. [13] developed a system that mediates privacy-preserving access to social relationships. It takes users' social relationship graph as an input, then it performs Random walking algorithm to obfuscate the social graph topology.

Recently, approximation of ℓ_1 distance has been used for privacy preserving in social networks. EWPM [14] is a protocol which provides a realistic matching approach considering both the number of common interests and the corresponding weights on them. P-match [15] has been proposed to privately match the similarity with potential friends in vicinity. P-match also considers both the number of common interests and the corresponding priorities on each of them individually. Ben has proposed Weighted Average Similarity (WAS) algorithm [16], which considers both the number of common interests and the corresponding weights on them, to protect users' privacy without reliance on any Trusted Third Party.

III. Preliminaries

In this section, some preliminaries about random walking and Paillier homomorphic encryption are briefly reviewed.

A. Truncated Random Walking Model

Since there is no direct attributes in our approach, another sort of attribute-like property to define the closeness between two users should be employed, that is results from random walking. So, some preliminaries about random walking model are briefly reviewed here.

Given social network graph $G=<V,E>$, where V is a vertex set representing the social network users, and E is edge set representing the social relationships between users. The adjacent matrix is denoted as B

$$b_{ij}=\begin{cases}1 & if <vi,vj>\in E\\ 0 & Otherwise\end{cases}$$

Then every node sends out W random walkers, and the random walker, who comes from user v_i, is denoted as w_i. And every random walker has a time-to-live (TTL) t, initially set to T, denoted as $w_{TTL}=T$, which represents the hops number of every random walker can walk on the social graph. Once a node receiving a random walker, he records the ID of w and deducts its TTL t, and sends it to a random neighbor if $t>0$. We generate the random connection matrix as follows:

$$\Pr\left(b_{ij}=1\right)=\begin{cases}\alpha & if\ b_{ij}=1\\ \beta & Otherwise\end{cases},$$

where $\beta=1-\alpha$. The corresponding random connection matrix is

$$B_R=\begin{pmatrix}\alpha & \beta & \alpha\\ \beta & \alpha & \beta\\ \alpha & \beta & \alpha\end{pmatrix}.$$

Then random walkers go on random walking until $t=0$.

B. Paillier Homomorphic Encryption

The Paillier homomorphic encryption secure computation consists of the following stages.

- Key generation: The Key Generation Center (KGC) chooses two large prime numbers p and q, and computes $N=pq$ and $\lambda=\mathrm{lcm}(p-1,q-1)$. It then selects a random $g\in\mathbb{Z}^*_{N^2}$ such that

$\gcd\left(L\left(g^{\lambda} \bmod N^2\right), N\right) = 1$, where $L(x) = \frac{x-1}{N}$. The KGC's Paillier public key is (N, g) and the private key is (p, q).

- Encryption: Let $m \in \mathbb{Z}_N$ be a plaintext and the ciphertext is given by $E_{\chi}(m) = g^m \cdot \chi^N \bmod N^2$, where $\chi \in \mathbb{Z}_N$ is a random number, and $E(\cdot)$ denotes the Paillier encryption operation.
- Decryption: Given a ciphertext $c \in \mathbb{Z}_{N^2}$. Then, the corresponding plaintext is given by

$$D\left(E_{\chi}(m)\right) = \frac{L\left(c^{\lambda} \bmod N^2\right)}{L\left(g^{\lambda} \bmod N^2\right)} = m \bmod N,$$

where $D(\cdot)$ denotes the Paillier decryption operation.

Note that the entity who executes decryption does not learn the value of χ used during encryption. The Paillier cryptosystem is probabilistic and semantically secure, because χ is chosen randomly for every encryption. The Paillier cryptosystem has two useful properties.

- Homomorphic. For any $m_1, m_2, \chi_1, \chi_2 \in \mathbb{Z}_N$, we have

$E_{\chi_1}(m_1) E_{\chi_2}(m_2) = E_{\chi_1 \chi_2}(m_1 + m_2) \bmod N^2$,

$E_{\chi_1}^{m_2}(m_1) = E_{\chi_1}(m_1 m_2) \bmod N_2$.

- Self-blinding.

$E_{\chi_1}(m_1) \chi_2^N \bmod N^2 = E_{\chi_1 \chi_2}(m_1)$, which implies that any ciphertext can be modified arbitrarily without knowing the plaintext.

IV. Construction of Privacy-Preserving Access Control

A. Pre-processing of Random Walking Results

Through the execution of random walking algorithm stated in Section III, every online social network user (denoted as node v_i) should collect a set of random walkers. According to the identities of random walkers, every node can count the amount of walker u_j issued by node v_j . Next, this node forms a random walker vector $\mathbf{u}$ with u_j, whose length is equal to $|V|$.

For example, a social network has 100 users, and user Alice has obtained a random walker set $\{3rw_1, 5rw_4, 1rw_5\}$, where $3rw_1$ represents 3 random walkers come from node v_1. Then the corresponding random walker vector of Alice can be formed as $\mathbf{u} = (3,0,0,5,1,0,\cdots,0)$, whose length is100, and the *i-th* element of vector $\mathbf{u}$ represents the amount of random walkers from v_i.

B. Computation of Closeness

With proper parameters W and T , the random walker issued by v_i will more likely reach other nodes which is more close to v_i. So that by inspecting the approximation of random walker vector $\mathbf{u}$ and $\mathbf{v}$, namely $\|\mathbf{u} - \mathbf{v}\|_1$, we can figure out how close node v_i is with another node v_j using ℓ_1 distance protocol [17].

Assume Alice is the resource owner and Bob is requestor. According to the random walk model described in section II, both of them have formed their own random walker vectors. The walker vectors of Alice and Bob are denoted as $\mathbf{u}$, $\mathbf{v}$ respectively. On one hand, Alice has to compute the approximation of vector $\mathbf{u}$ and $\mathbf{v}$ to determine how they are close before she permits Bob's request; On the other hand, to prevent the privacy of Bob, $\mathbf{v}$ should not be presented to Alice directly. Fortunately, Paillier homomorphic encryption [18] can be used to deal with this dilemma.

Since Alice and Bob have the corresponding random walker vectors $\mathbf{u} = (u_1, u_2, \cdots, u_n)$ and $\mathbf{v} = (v_1, v_2, \cdots, v_n)$, and we have

$$\|\mathbf{u} - \mathbf{v}\|_2^2 = \sum_{i=1}^{n} (u_i - v_i)^2 = \sum_{i=1}^{n} \left(u_i^2 + v_i^2 - 2u_i v_i\right).$$

One can see that Alice knows $\sum_{i=1}^{n} u_i^2$, Bob knows $\sum_{i=1}^{n} v_i^2$, but $\sum_{i=1}^{n} (-2u_i v_i)$ contains the cross terms and is unknown to both of Alice and Bob. For secure computation, Alice generates a public/ private key pair and shares only public key with Bob. Alice and Bob will follow the steps of the protocol for secure computation of the squared ℓ_2 distance as below.

For every $i \in (1,2,\cdots,n)$, Alice encrypts u_i into $E_{\chi_i}(u_i)$ according to the encryption process of Paillier cryptosystem. Here, $\chi_i \in \mathbb{Z}_N^*$ is chosen randomly. Then Alice transmits the encrypted vector $E_{\chi}(\mathbf{u})$ to Bob.

For every $i \in (1,2,\cdots,n)$, Bob computes

$$E_{\chi_i}^{-2v_i}(u_i) \bmod N^2 \equiv E_{\chi_i}(-2u_i v_i).$$

Bob computes

$$E_{\chi_C}\left(\sum_{i=1}^{n} (-2u_i v_i)\right) \equiv \prod_{i=1}^{n} E_{\chi_i}(-2u_i v_i) \bmod N^2,$$

where $\chi_C = \prod_{i=1}^{n} \chi_i \bmod N \in \mathbb{Z}_N^*$. Note that Bob operates solely in the encrypted domain in this step, so the values of $\sum_{i=1}^{n} (-2u_i v_i)$ and χ_C are unknown to him.

Bob chooses $\chi_B \in \mathbb{Z}^*_N$ randomly, and $\chi_D = \chi_B \chi_C \bmod N \in \mathbb{Z}^*_N$. Then, he computes

$$E_{\chi_D}\left(\sum_{i=1}^{n} v_i^2 + \sum_{i=1}^{n}(-2u_i v_i)\right) \equiv E_{\chi_B}\left(\sum_{i=1}^{n} v_i^2\right) E_{\chi_C}\left(\sum_{i=1}^{n}(-2u_i v_i)\right) \bmod N^2$$

Bob transmits this result to Alice. One can see that the value of χ_D is implicit in the encryption result but is unknown to Bob, since he does not know the value of χ_C.

Alice chooses $\chi_A \in \mathbb{Z}^*_N$ randomly and $\chi = \chi_A \chi_D$, then she computes

$$E_{\chi}\left(\|\mathbf{u}-\mathbf{v}\|_2^2\right) = E_{\chi}\left(\sum_{i=1}^{n}\left(u_i^2 + v_i^2 - 2u_i v_i\right)\right)$$
$$\equiv E_{\chi_A}\left(\sum_{i=1}^{n} u_i^2\right) E_{\chi_D}\left(\sum_{i=1}^{n} v_i^2 + \sum_{i=1}^{n}(-2u_i v_i)\right) \bmod N^2$$

Note that, the value of χ is also implicit in the encryption result but unknown to Alice because she does not know the value of χ_B.

Alice decrypts $\sum_{i=1}^{n}\left(u_i^2 + v_i^2 - 2u_i v_i\right) = \|\mathbf{u}-\mathbf{v}\|_2^2$ using the private key according to the decryption process of Paillier cryptosystem.

We can see that, this protocol does not reveal $\mathbf{v}$ to Alice or $\mathbf{u}$ to Bob.

C. Decision on Request

After the execution of computation of closeness, Alice would obtain the value of $\|\mathbf{u}-\mathbf{v}\|_2^2 \approx \|\mathbf{u}-\mathbf{v}\|_1$. Then, she can make the decision by checking whether $\|\mathbf{u}-\mathbf{v}\|_1 \le \tau_A$, where τ_A is a permissible threshold set by Alice herself. If yes, she will allow Bob to access her data. Otherwise, she declines the request.

V. Implementation and Evaluatuon

A. Data Sets and Preparation

We have implemented a preliminary prototype of the proposed scheme, which provides access control with privacy preserving. We use the Facebook friendship graph from the New Orleans regional network [20] to simulate the social graph in our scheme. This dataset describes the links between users from the Facebook New Orleans network, consisting of 63,732 nodes and 1.545 million edges. To show our experiment results clearly, only 100 access requests are shown.

B. Results

Three parameters (W, T, τ_i) need to be set initially before the experiments, where W is the random walker number of every node have issued, T represents time-to-live (TTL) of every random walker, and τ_i is the permissible threshold value set by node v_i.

TABLE I. Approximation from ℓ_1 Distances

1	6	26	12	51	12	76	2
2	8	27	3	52	14	77	16
3	1	28	12	53	12	78	14
4	7	29	20	54	18	79	20
5	10	30	14	55	14	80	8
6	12	31	3	56	17	81	12
7	9	32	12	57	8	82	9
8	16	33	8	58	17	83	14
9	1	34	16	59	2	84	3
10	18	35	3	60	10	85	17
11	2	36	14	61	12	86	18
12	15	37	16	62	4	87	14
13	6	38	7	63	17	88	10
14	4	39	17	64	5	89	3
15	9	40	10	65	20	90	16
16	14	41	3	66	16	91	17
17	1	42	17	67	4	92	10
18	10	43	1	68	1	93	17
19	14	44	17	69	14	94	14
20	9	45	5	70	15	95	18
21	12	46	20	71	17	96	8
22	4	47	10	72	8	97	12
23	8	48	8	73	1	98	16
24	14	49	12	74	16	99	1
25	1	50	18	75	12	100	12

Note that, in order to investigate how much the variation of parameters would affect the access control, we also set the value of τ uniformly. When setting $W = 10$ and $T = 10$, we have obtained100 approximation of ℓ_1 distances, who are shown in Table I.

We employ a variety of parameters combination to observe the influence on results. Firstly, we set $(W, T, \tau_i) = (10, 10, 5)$, the outcome is shown as in Fig.2, which depicts the number of passed the closed-relationship verification of access requests, such as the first dot in Fig.2 represents two pairs of nodes could pass the access control when there are ten access requests.

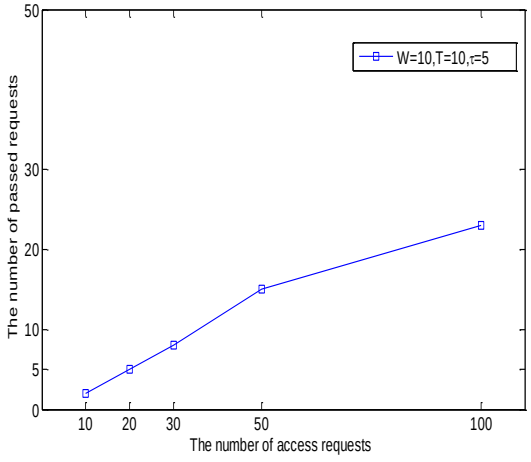

Fig. 2. The number of passed the closed-relationship verification of access requests

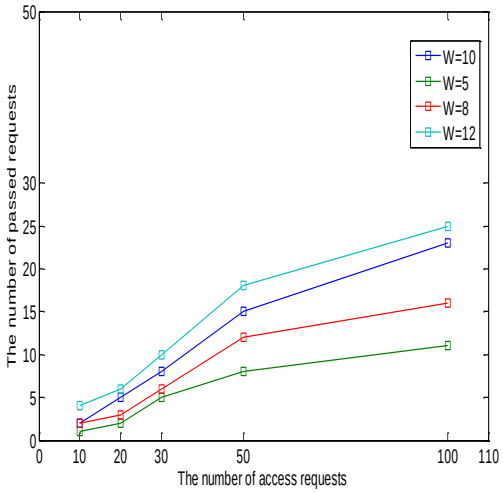

Fig. 3. The number of passed the closed-relationship verification influenced by W

To figure out how much parameter W would affect the access control, we vary the value of W while keep T and τ stable. We set $(W,T,\tau)=(5,10,5)$, $(W,T,\tau)=(8,10,5)$ and $(W,T,\tau)=(12,10,5)$. As shown in Fig.3, the amount of passed requests is consistent with the variation of parameter W. This phenomenon is in accordance with our theoretical study. If W decrease, the amount of collected random walkers by every node would decrease as well. Since the number of common random walker is smaller, the amount of passed requests would be smaller than before when it proceeds to the computation of closeness.

Next, we investigate the influence from T .we set $(W,T,\tau)=(10,5,5)$, $(W,T,\tau)=(10,15,5)$ and $(W,T,\tau)=(10,20,5)$. The outcome shows as in Fig.4.

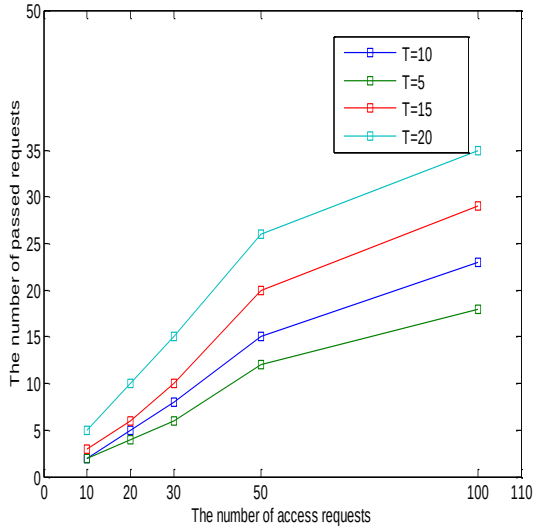

Fig. 4. The number of passed the closed-relationship verification influenced by T

One can see that the variation of the amount of passed requests is also consistent with the variation of parameter T. However, we have observed that the influence from T is much smaller than W 's when we decrease the same value of W and T. This is caused by chose relationship. So we have increased variation of T.

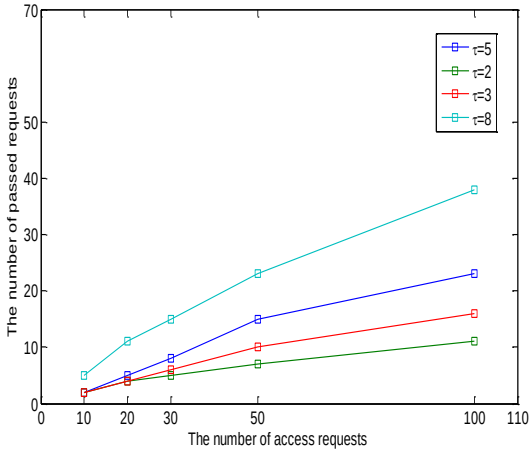

Fig. 5. The number of passed the closed-relationship verification influenced by τ

At last, we vary the value of parameter τ. We set $(W,T,\tau)=(10,10,2)$, $(W,T,\tau)=(10,10,3)$ and $(W,T,\tau)=(10,10,8)$. Fig.5 depicts the variation of the amount of passed requests is in the opposite trend of τ 's variation. This result is also consistent with our theoretical analysis. Although the amount of random walkers remains unchanged, when set the permissible threshold τ to a smaller value, this means only those has much closer relationship with the owner can be allowed to access, so that the number of passed requests is smaller than before.

Adamic et al. [21] has proposed a classical scheme (Adamic-Adar for short) to measure similarity between two users, and their scheme is based on common neighbors and the degrees of those common neighbors. The formulation expression of Adamic/Adar is:

$$Similarity(u,v)=\sum_{i\in\Gamma(u)\cap\Gamma(v)}\frac{1}{\lg|\Gamma(i)|},$$

where $\Gamma(i)$ denotes the set of neighbors of node i in social graph. We have employed Adamic-Adar to evaluate the accuracy of our scheme. To find out which parameters setting is more practical for our proposed scheme in reality. We have counted the distribution of the similarity value in Adamic-Adar and our scheme. We have sampled the first ten percent, the middle ten percent and the last ten percent of the 100 similarity values to compare our scheme clearly.

After executing our scheme and computing the similarity of node pairs according to Adamic-Adar, we get the best parameter setting shown as in Fig.6. One can see that the accuracy of our scheme is almost equal to the outcome of Adamic-Adar scheme when setting $W=10,T=10$.

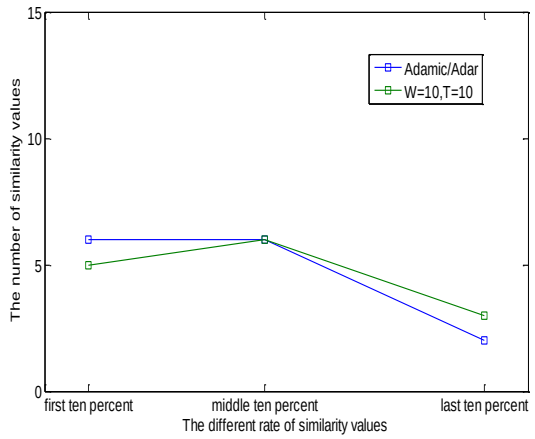

Fig. 6. The best parameter setting

VI. Conclusion

In this paper, a random walk based access control scheme is investigated in this paper. . The proposed novel approach employs random walking to form the profile for online social users. In terms of the formed profile, users can carry out access control according to the secure computation of closeness. Furthermore, the user can set the permissible threshold independently according to his access policy. In this way, the leakage of privacy existing in traditional attribute based access control has been removed. Experimental results show that the proposed scheme is reasonable and practical. In our future work, more efficient approach for computation of closeness will be investigated.

Acknowledgement

This work was jointly supported by the National Social Science Foundation of China (no. 14CTQ026), the National Natural Science Foundation of China (no. 61472464), the Chongqing Research Program of Application Foundation and Advanced Technology (no. cstc-2014jcyjA40028, no. cstc-2013jcyjA40017), the Natural Science Foundation of Shandong Province, China (no. ZR2015FL024).

Reference

[1] BCarminati, E Ferrari, M Viviani. Security and trust in online social networks[J]. Synthesis Lectures on Information Security, Privacy, & Trust, vol.4, no.3, pp.1-120, 2013.

[2] R. Shantanu, S.Wei and V. Anthony,"Privacy-preserving approximation of L1 distance for multimedia applications," Multimedia and Expo (ICME), 2010 IEEE International Conference, Singapore,pp. 492-497, 2010.

[3] S.R.Kruk, S.Grzonkowski, A.Gzella, T.Woroniecki andH.C.Choi, "DFOAF: distributed identity management with access rights delegation,"In The Semantic Web–ASWC 2006, Springer Berlin Heidelberg, pp.140-154,2006.

[4] B.Ali, W.Villegas and M.Maheswaran,"A trust based approach for protecting user data in social networks,". In Proceedings of the 2007 conference of the center for advanced studies on Collaborative research,IBM Corp, pp.288-293, 2007.

[5] B.Carminati, E.Ferrari and A.Perego,"Security and privacy in social networks," Encyclopedia of information Science and Technology, pp 3369-3376, 2008.

[6] D. Brickley andL. Miller, "FOAF vocabulary specification 0.91," Available at, http://xmlns.com/foaf/0.1, 2007.

[7] H.C.Choi, S.R. Kruk, S.Grzonkowski, K. Stankiewicz, B.Davids andJ.G Breslin,"Trust models for community-aware identity management," IRW2006/WWW2006 Workshop, 2006.

[8] B. Carminati, E. Ferrari and A. Perego,"Enforcing access control in webbased social networks,"ACM Transactions on Information and System Security (TISSEC), 13(1), 6, 2009.

[9] C. Barbara, F. Elena, H. Raymond, K. Murat andT. Bhavani, "Semantic web-based social network access control," Computers & Security In ELSEVIER, pp. 108-115, 2011.

[10] Y.Y.Fu, M. Zhang, D.G.Fengand K.Q. Chen,"Attribute privacy preservation in social networks based on node anatomy,"RuanJianXueBao/Journal of Software, pp. 768−780, 2014.

[11] H.Pili, S.M.C Sherman, C.L. Wing,"Secure friend discovery via privacy-preserving and decentralized community detection," In ICML 2014 Workshop on Learning, Security and Privacy, 2014.

[12] D.Gabor and J. Mark, "Fully distributed privacy preserving mini-batch gradient descent learning," International Federation for Information Processing, pp. 30-44, 2015.

[13] L. Changchang and M. Prateek,"LinkMirage: Enabling privacy-preserving analytics on social relationships," In NDSS, 2016.

[14] Z.Xiaoyan, L.Jie, J. Shunrong, C. Zengbaoand L. Hui, "Efficient weight-based Private Matching for proximity-based mobile social network," In IEEE ICC, 2014.

[15] N.Ben, Z. Xiaoyan, Z. Tanran, C. Haotian and P. Hui,"P-match: Priority-aware frirnd discovery for proximity-based mobile social networks," In 2013 IEEE 10th International Conference on Mobile Ad-Hoc and Sensor Systenms,Hangzhou, pp. 4114-4119, 2013.

[16] L.Ben, Z. Xiaoyan, L. Jie, L. Zan and L.Hui,"Weight-aware private matching scheme for proximity-based mobile social network," In Globecom 2013- Symposium on Selected Areas in Communications, pp. 3170-3175, 2013.

[17] W.Du, M. Atallah and F. Kerschbaum,"Protocols for secure remote database access with approximate matching,"the 7th ACM Conference on Computer and Communications Security, Athens, pp. 523–540, 2000.

[18] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," in Advances in Cryptology, EUROCRYPT 99. 1999, vol. 1592Springer-Verlag, Lecture Notes in Computer Science, , pp. 233–238, 1999.

[19] W. B. Johnson and J. Lindenstrauss, "Extensions of Lipschitz Mapping Into Hilbert Space,"Contemporary Mathematics, vol. 26, pp. 189–206, 1984.

[20] B.Viswanath, A. Mislove, M. Cha and K.P. Gummadi,"On the evolution of user interaction in Fcaebook,". In Proceedings of the 2nd ACM SIGCOMM Workshop on Social Networks, Barcelona, pp. 37-42, 2009.

[21] L.A Adamic andE. Adar,"Friends and neighbors on the Web,"Social Networks, 25(3), pp. 211–230, 2003.