International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 15 (2017) pp. 5308-5317

New Model to evaluate User Reliability Dynamically for Social Network Services

Youngsook Lee*, Younsung Choi*, Changhoon Lee and Dongho Won*****

**Department of Cyber Investigation Police, Howon University, 64, 3-gil, Gunsan, Jeollabuk-do, 54058, Republic of Korea.*

***Information Technology Head Division , Nonghyup Bank, 59, Seonggogae-ro, Uiwang-si, Gyeonggi-do, Republic of Korea.*

****Department of Computer Engineering, Sungkyunkwan University, 2066 Seoburo, Suwon, Gyeonggido 440-746, Republic of Korea.*

Abstract

With the rapid propagation of smart devices, the Social Networking Service (SNS) has become the most popular service in IT industry. In SNS, there is no classification between information producer and consumer, but all participants can produce new information or use information freely. According to a recent e-marketer's report, about 1.2 billion people in the world use one or more SNSs. However, with this dramatic growth, various adverse effects have been reported: for example, impersonation, unproven rumours, online personal attack, and exposure of privacy. A girl in America even killed herself because of personal attacks on an SNS. To prevent these adverse effects of the SNS, moral advancement of SNS users is naturally the best solution; however, this goal is practically very hard to achieve. Therefore, another solution is demanded, since the SNS has already become an essential service in our lives. For these reasons, this paper proposes a new model to dynamically evaluate user reliability for SNSs. The purpose of our new model is to quantify user reliability, and to provide it to all participants. Based on this quantification, an SNS user can easily determine who is good or bad, and then makes a good relationship or bans bad people. Consequently, our new model provides a criterion in the building of online relationship, and we expect that our new model may replace authentication procedure.

Keywords: SNS, Reliability evaluation, SNS security, Privacy protection

INTRODUCTION

As the number of SNS subscribers rapidly increases, and the service is being magnified as the principal means of sharing information these days, social interest in SNSs is also increasing. Unlike single-way media, such as TV, newspaper and radio, in which the information producer delivers information to consumers in one direction, SNSs are bidirectional media that enable all users to directly produce, process and distribute information, without distinction of producer and consumer. SNSs are spreading rapidly for their simple process of production, and convenience in sharing with surrounding people. Sharing everyday life as well as obtaining and exchanging information through SNSs has become routine, and SNSs have been utilized for a range of purposes, as users increase in number, and form a collective intelligence. Due to expansion of the spread of smart devices, SNSs have become accessible to users everywhere through mobile devices, so it is expected that the number of users will increase much more, and their social impact will increase. As SNSs have become forums for sharing information, many problems have arisen, for example, exposure of information, spread of false rumour, and impersonation.

Because a large amount of information that information producers produce is obscure, and such information indiscriminately proliferates, users experience difficulty in judging the reliability of information within the service, and damage due to false information has occurred on a continual basis. Also, the unintended spread of information causes invasion of privacy, as a result of sharing sensitive personal information with a majority of people, and the problem of lowering the reliability of service, through damaging others by disguising one's identification, or making multiple accounts, so that making ill use of the online environment is also widespread. Accordingly, there is a need to evaluate the reliability of a node (in this paper, a node denotes a person in an SNS), that is to say the user account, which is an information producer, to cope with the problem. It becomes possible to judge the reliability of information according to the reliability of the node, and prevent damage by false information or threat, caused by a false account. Through the

reliability of a node, a standard to judge the reliability of information is established for service users, and users are able to selectively share information, by identifying the reliability of a node when they wish to share sensitive information. Enabling information producers to deliver information only to a person they want to share with, and limiting the people who can receive that information, can be the method to minimize damage from invasion of privacy.

What should be considered when suggesting a countermeasure for the problem of invasion of privacy is that openness, which is one of the main characteristics of SNSs, should not be damaged. SNSs have been able to spread rapidly, thanks to openness of information; and such openness can be considered a driving force of SNSs. However, due to such openness, problems such as invasion of privacy have occurred, so a measure to combine those two elements of openness and privacy is necessary as well. When a person shares his or her information, filtering for a person he or she wishes to share with is necessary, and reliability can be considered its criterion. Public information can be confirmed by everyone, but information sensitive to a person shall be delivered only to a person whom the information producer puts their trust in. For the foregoing needs, a variety of methods have been suggested to judge the reliability of a node in SNSs. However, previous researches as [1], [4]-[15] have suggested methods that evaluate and verify reliability, by extracting common features on the basis of profile information of a node of personal information; and a method that gives shape to an abstract concept of trust, and realizes it on the social network, has not yet been suggested. Trust among people is a continuously changing element, not a fixed one, and a dynamic user reliability evaluation scheme that evaluates reliability, considering changeability, is necessary.

This paper suggests both a definition of reliability, and a scheme capable of expressing a relation with a person who gains trust, not only in SNSs, but in reality, through mapping with a function that is commonly provided in SNSs. The structure of this paper is as follows. Section 2 analyses the definition of SNSs and security threats through related research, and defines reliability, by analysing the confines of existing research. Section 3 of this paper suggests a dynamic user reliability evaluation scheme, by mapping parameters with functions of SNS, according to the definition of reliability. Section 4 addresses the advantages of the proposed scheme, while Section 5 presents a conclusion to this paper.

PRELIMINARIES

A. Definition of SNS and Security Threat

An SNS is a service model that creates and distributes information on the basis of user relationships. Users can create information easily by themselves, and share information with a social group they belong to, by platform. They are also able to exchange the information, as well as correct and disseminate it freely in real time. Due to the advent of SNSs that enable free communication, without restriction of time and space, the production and distribution of knowledge and information have changed from service provider-centered, to consumer-centered. In an SNS, general users share their everyday life with others, or set forth their views on the latest issue, have discussions with others in real time, and acquire, as well as exchange information, on their interests, hobbies, etc. From the corporate aspect, SNSs are used to analyse consumers' requirements, and broadcast corporations are utilized by government agencies as channels to listen to people's voices, and communicate with people.

However, as the number of users of SNSs increases and the service is more widely used, the security threat continuously increases as well. A great number of vulnerabilities inherent in the service exist, due to the open characteristics of SNSs, and malicious attackers cause damage to users and services, and lower reliability, by making wrong use of the vulnerabilities. Attacks may occur after collecting a user's profile and other personal information, by creating a new account, using a weak point of service authentication, or spreading false information by creating multiple false accounts. In addition, there is a threat of invasion of privacy through the unintended spread of information, or spamming, by making ill use of collected data, and a great number of users may attack and lower reliability, by spreading false information with malicious intention. [Table 1] shows the kinds of security threat that may occur in an SNS [2].

Security threats afflict users, and result in a lower reliability of service, by making ill use of the characteristics of SNSs that seek openness of information, according to the relationship. To cope with such threat, an index that enables users and service to evaluate the reliability of a node is necessary.

B. Confines of Existing Researches

Researches for the protection of privacy and improvement of reliability in SNSs are actively conducted at home and abroad, and privacy protection technology or reliability evaluation schemes are also being suggested, for application to SNSs.

However, definition of the standards of reliability among people offline is not evident in the existing research, and the methods for finding common features between nodes, and judging reliability by analysing their common features according to fixed information, such as profile information, have instead been suggested. Those theses aim to suggest a standard for making a judgment on whether or not a person is reliable, by calculating the reliability with an unrelated person.

But the confines of existing researches lie in whether or not a node is reliable only by the fact that there is a mutually related element in the profile. For example, a person who lives in the

same area, and works at the same company, after graduating from the same school, and joining the same club with a similar hobby, may not be that person at all; or even if the person is one the user knows by chance, the user cannot guarantee that the common element shown in the profile is reliable.

Therefore, to protect privacy, and judge reliability, there is a need to evaluate dynamic reliability that reflects time and situation, not static reliability that uses only fixed elements. This paper suggests the definition of reliability, and a dynamically changing user reliability evaluation scheme, by mapping a parameter with the function of an SNS, after drawing a trust parameter from the definition of reliability. The suggested scheme can be used as a measure capable of judging the reliability of a person involved, by continuously reflecting the changes of time and situation, after building relationships with the people in the SNS

Table 1. Security threat in SNSs

Classification	Security Threat	Content
Authentication	Identity theft attack	Attack masquerading as the owner of identity information, by obtaining the identity information of an actual user for malicious purposes.
	Sybil attack	Attack to reduce the reliability of service, and to forge a reputation based on a large quantity of false identity information generated by a malicious attacker.
	Reputation bleaching	Malicious action of newly registering to the system to get a new identity if the user has a lower reputation than the new reputation that user gets when first joining the system.
Privacy	Unauthorized Data Collection	Attack using information for malicious purposes or commercial purposes, by collecting the profile information of users on an SNS.
	Privacy bleaching	Attack taking place as an invasion of privacy in a way that is not intended. Information published on an SNS is spread by other users, who have established relationships with the information's owner.
Others	Spam on social web	Attack spreading spam data by directly making, or participating in the dissemination of spam generated by malicious users. Malicious action intentionally spreading a negative reputation, and exaggerated information about a product or brand of a specific person.
	Eclipse attack	Attack reducing the reliability of service, and forging the reputation of a normal user, by spreading false information, by making an actual user with malicious intent.

C. Confines of Existing Researches

With respect to reliability, Fukuyama defines reliability (trust) as "The expectation that arises within a community of regular, honest, and cooperative behaviour, based on commonly shared norms, on the part of other members of that community" [3]. In other words, reliability can be the expectation that trust in people is created by following universal norms and rules, and sharing common value, and such behaviours will continue on a regular and repetitive basis. The standard of thinking that we trust a person according to the definition of reliability is that we judge that we trust a person who observes norms, the directivities of shared value are similar to each other, and the degree of sharing each value is considered to affect reliability.

Adhering to norms means a person who is well adapted to a given environment and organization, and connotes that he or she does not have any malicious intention toward others. Because a person who keeps norms well is expected to be moral and ethical, people generally put their trust in a person who observes norms.

Similarity in the directivity of shared value means that ideas are similar to each other. Cooperative behaviour means pursuing a similar value, and behaving together, by establishing the same objective and purpose. People put faith and believe more in a person who behaves in a similar fashion with similar value, rather than in disparate ones. In addition, it

can be an important factor in forming confidential relationships between people, as it enables people to exchange similar values and thoughts with each other.

The degree of exchange indicates the intimacy in a relationship, and the index is considered to play a role as verifier, to judge whether or not the other party is more reliable. The degree of exchange is also closely related to the observance of norms and similarity in value. In most cases, people wish to maintain close relations with an honest person who observes norms, rather than one who is dishonest, and maladjusted to the environment. Also, when values and ideas are similar to each other, people can share information and exchange their thought frequently, which naturally makes the level of intimacy increase. Therefore, the degree of exchange has a close relationship with the other two elements, and intimacy means to verify the two elements. It can be said that the more people engage in mutual exchange, the more intimacy rises, and reliability proportionally increases.

The degree of evaluation and exchange in respect of reliability with persons in real life is intrinsically similar in SNSs. Therefore, it is possible to form a dynamic user reliability evaluation scheme, by mapping the standard with the function of the SNS.

NEW MODEL TO EVALUATE USER RELIABILIY DYNAMICALLY FOR SNS

In this section, we describe our proposed scheme, which dynamically evaluates user reliability in SNS. Before describing the proposed scheme, we define notations used in the proposed scheme. Figure 1 depicts the environments of the proposed scheme and its notations.

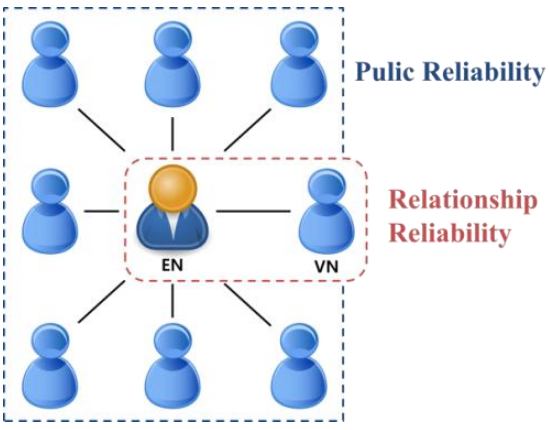

Figure 1: Reliability on SNS environments

Figure 1 shows two types of nodes: verifying node and evaluated node. Verifying node (VN) is a node that wants to compute the reliability of the target node (Evaluated Node, EN). The reliability consists of two reliabilities: public reliability and relationship reliability. Relationship reliability is computed based on three parameters, N, V, and F. Relationship reliability only applies between VN and EN. Therefore, parameters N, V, F show similarity between two nodes. However, if VN has not met EN before, online similarity checking is not sufficient to trust EN, so public reliability is necessary. Public reliability is the reputation of EN. The combination of relationship reliability and public reliability make it easy for VN to determine whether EN is trustworthy or not. The following subsection provides detail description of parameters N, V, and F.

A. Trust Parameters

In the suggested scheme, each user account is a node, and when assuming a node for which reliability has been evaluated as EN, and a node that confirms the reliability of EN as VN, the total reliability is classified as public reliability and relationship reliability. Public reliability is defined as open reliability toward a set of entire nodes that the EN is entering into a relation with in an SNS, and it is expressed as P. Relationship reliability is defined as the personal reliability between EN and VN, in which all nodes other than EN and VN are excluded, that is to say the mutual reliability between individual and individual in an SNS, which is expressed as R. Here, public reliability has objectivity, as the evaluation of the majority is expressed; whereas relationship reliability reveals the subjective characteristic compared to public reliability, as it is mutual evaluation between individuals [11-15].

The reason for disentangling public reliability from relationship reliability is that VN is a situation that verifies the reliability of EN, so relationship reliability, which is the reliability evaluation factor between the two, is used; but because evaluation only by relationship reliability that evaluates simply according to value similarity and degree of exchange between two nodes of EN and VN may be subjective, there is a very strong possibility of making a mistake in the evaluation of reliability. Thus, public reliability is included, due to the necessity to reflect the intention of the entire group involved, to secure objectivity of evaluation.

Public reliability and relationship reliability comprise three parameters, according to the definition of reliability. The first parameter is the degree of observance of norms (N). As a parameter to judge how well a person observed conventional norms within the service in a given time, it is the numerical value of how well a person abided by the rules and norms of service during the time (t) from a specific point of time of the past to the present point, since judgment on the observance of norms and rules, and honesty is available. A point to be considered due to the nature of the service is that following the norms and rules must not be a hindrance to the production of information, as it is needed to minimize the openness of an SNS. Because it must not be dominated by a specific idea or

subjective thought, and should be the norms stemming from objective and conventional thought, the norms and rules shall guarantee the freedom of thought and expression, but be limited to the words and behaviours that do not offend against common decency, such as information slandering others, damaging others' reputation, and causing damage to others. Service functions mapped with the parameter N include cut off relations or reports by the other user, and filtering due to the use of negative language, such as swearing. When relations are blocked, or reported by others due to words or information causing damage to others, the N value declines, as it is judged as an act causing damage to the user and service. However, as to the applicable elements to prevent wilful reports, or cut-off by a malicious user, the service provider is required to provide an environment to enable the SNS to be normally used, by setting a limit, or giving a warning in case it is especially high, as a result of investigation of the frequency of each node. When using negative language such as swearing, the N value also declines, as it is regarded as an act that damages another's reputation, and causes damage. Because N is a numerical value to judge whether or not all people observed norms within the same period of time, the value decreases on a gradual basis, when breaking norms based on the default value D. The parameter N is expressed as Equation (1).

$$N = D - \frac{1}{h}\sum_{k=1}^{h} n_k \quad (1)$$

The degree of norm observance in public reliability and relationship reliability is expressed as N_p and N_r, respectively. As the number of service functions is discretionally adjustable, according to the value of h, the addition or exclusion of appropriate function is available per the respective service.

The second parameter is the degree of value similarity (V). As a parameter to judge whether or not value and thought in respect of shared writing and information are similar to other users, the numerical value has a sense of similarity, and increases when sharing information that arouses sympathy. Among the functions of service that are mapped with parameter V are recommendation, clipping (copying), and a group member belonging to the same group. The parameter increases when there is an interaction with respect to information, such as another's recommendation and clipping, and the value of V may increase, when it belongs to the same group in the service. Parameter V is expressed as Eq. (2).

$$V = \frac{1}{h}\sum_{k=1}^{h} v_k \quad (2)$$

The degree of value similarity in public reliability and relationship reliability is expressed as V_p and V_r, respectively.

The third parameter is the degree of information exchange (F). Frequent mutual exchange shows high intimacy and necessity, makes intimacy increase on a continual basis, and sharing information becomes the means of confirming the other party's thoughts and intentions, so parameter F affects the evaluation of reliability. The functions of service that are mapped with Parameter F include frequency of visit, comment, message, note, and chatting. There is a correlation between those elements and intimacy, and the more intimacy increases, the more reliability proportionally increases as well. Parameter F is expressed as Eq. (3):

$$F = \frac{1}{h}\sum_{k=1}^{h} f_k \quad (3)$$

The degree of information exchange in public reliability and relationship reliability is expressed as F_p and F_r, respectively. When considering functions that are commonly provided by a variety of SNSs, the table for trust parameter and mapping of the service function is the same as Table 2.

Table 2: Mapping table

Trust Parameter	**Function**
Degree of observance of norms (N)	Cut off relation (n_1), Report (n_2), Swearing filtering (n_3)
Degree of value similarity (V)	Recommendation (v_1), Clipping (v_2), Group member belonging to the same group (v_3)
Degree of information exchange (F)	Frequency of visit (f_1), Comment (f_2), Message (f_3), Note (f_4), Chatting (f_5)

B. Dynamic User Reliability Evaluation Scheme

The notations used throughout this paper are summarized in Table 3.

Table 3: Notation

Notation	**Description**
T	Total reliability
P	Public reliability
R	Relationship reliability
N_p / N_r	Degree of observance of norms (public / relationship)
V_p / V_r	Degree of value similarity

	(public / relationship)
F_p / F_r	Degree of information exchange (public / relationship)
a_p / a_r	Norms coefficient (public / relationship)
b_p / b_r	Similarity coefficient (public / relationship)
c_p / c_r	Exchange coefficient (public / relationship)
m_p	Weighted value of public reliability
n_r	Weighted value of relationship reliability

The value of trust parameters varies on a continual basis, according to the time of service use and the degree of utilization, so a dynamic user reliability evaluation scheme capable of evaluating the reliability of each node in an SNS is realizable by using the parameter. As the public reliability P shows the average reliability evaluated by the nodes that built a relationship with EN, when setting the number of entire EN-related nodes as n, the public reliability P can be expressed as the sum of reliability of nodes. Therefore, public reliability can be calculated with the following Eq. (4):

$$P = \frac{1}{n}\sum_{k=1}^{n} P_k \quad (4)$$

Pk refers to the reliability of each node that entered into a relation with EN. Pk is expressed as Eq. (5):

$$R_k = a_p N_{pk} + b_p V_{pk} + c_p F_{pk} \quad (5)$$

P_k can be calculated as the sum of trust parameters, and in Eq. (5), ap, bp and cp are constants showing the weighted value of respective trust parameters in public reliability. They are expressed as norms coefficient a_p, similarity coefficient b_p, and exchange coefficient c_p, respectively. By Eqs. (4) and (5), the public reliability P can be expressed as Eq. (6):

$$P = \frac{1}{n}\sum_{k=1}^{n}(a_p N_{pk} + b_p V_{pk} + c_p F_{pk}) \quad (6)$$

As relationship reliability R is the subjective reliability of VN that evaluates EN, it can be expressed as Eq. (7), analogous to the method that expresses the reliability of a node in Eq. (5):

$$R = a_r N_r + b_r V_r + c_r F_r \quad (7)$$

The relationship reliability R can be calculated as the sum of trust parameters, and in Eq. (7), a_r, b_r and c_r are the weighted value of trust parameters in relationship reliability, which are expressed as norms coefficient a_r, similarity coefficient b_r, and exchange coefficient c_r.

The reliability of EN evaluated by VN is the total reliability (T). It is possible to derive the value of total reliability of EN evaluated by VN, from the values of public reliability P and relationship reliability R. The total reliability is expressed as Eq. (8):

$$T = \sqrt{(m_p P)^2 + (n_r R)^2} \quad (8)$$

where, the proportional constants showing the weighted value of public reliability and relationship reliability, m_p and n_r in Eq. (8) show the weighted values of public reliability and relationship reliability, respectively. The values of m_p and n_r in Eq. (8) should satisfy $m_p{}^2 + n_r{}^2 = 1$, to maintain consistency of average of the value of total reliability, even in case the values of the two vary. Accordingly, the values of m_p and n_r are the same as in Eq. (9):

$$m_p = \cos\theta, n_r = \sin\theta \quad (9)$$

(However, m_p and n_r are positive numbers, and $0 \le \theta(\text{Theta}) \le \frac{\pi}{2}$)

It is possible to adjust the weight of public reliability and relationship reliability, by modifying the values of m_p and n_r

ANALYSIS FOR PROPOSED DYNAMIC MODEL

In this section, we compare the existing SNS access control policy and the proposed scheme. According to the comparison, we prove the proposed scheme is more secure than the existing one, and offers advantages.

A. Limitations of the existing SNS access control policy

Currently, many SNSs are worldwide services, and each SNS has its own access control policy. However, many of the access control policies are similar, because the design of access control policy is simple. We refer to the access control policy of Facebook, which is the most popular SNS in the world. Table 4 explains the access control policy of the user contents in Facebook.

This policy has the limitation that users cannot set access control policy in detail. Actually, we meet and part from many friends during life, and some of them are not familiar enough to share privacy with, or are uncomfortable to do so. In particular, if a user wants to share his/her contents with very familiar friends, rather than normal friends, the existing access control policy cannot support this case. In short, the existing access control policy forces all or nothing on users. In addition, users in SNS have no right to define access control policy, and just obey the policy set by the service provider,

though his or her contents are the origin and basis of the SNS.

Table 4: Access control policy of the Facebook

Access control policy	Description
Public	Contents having this option will be open to all people who use Facebook.
Friend only	Contents having this option will be only open to friends set by the user in Facebook.
Only Me	Contents having this option will not be open, and only the user who creates this content can access the content.
Custom	Contents have this option will be open to persons chosen by the user in Facebook. The user, the contents owner, can choose persons in three groups: friends, friends of friends, and specific people.

B. Advantages of the proposed model

The proposed scheme has two advantages. Firstly, the proposed scheme provides a more detailed access control policy than the existing one. Secondly, the user can make his or her own access control policy in the proposed scheme. This means that the initiative of making access control policy moves from service providers to users. We now address these advantages in detail using an example. For explanation, refer to Figure. 2.

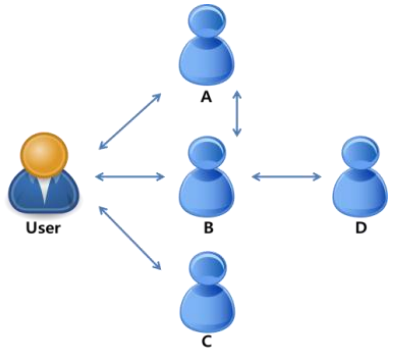

Figure 2: A situation for example

Figure 2 shows a user has three friends; A, B, and C. A and B are friends to each other. D has no connection with the user, but D is a friend of B. So D is a friend of friends to the user. To compute the reliability of each user, we assign various features to each entity. Table 5 shows the features of each entity in Figure. 2

Table 5: Features of each entity in figure 2.

Entity	Features
User	Education : Gunsan high school, Howon University , Address : Gunsan, Jeonrabuk-Do, Korea Hobby : Football , Inclination of politics : Progressive
	Groups in SNS : Football, Howon University Frequency of communication with A in SNS : about 10 times a day Frequency of communication with B in SNS : about 8 times a day Frequency of communication with C in SNS : about 2 times a day
	Have no experience to ban others user or banned by other users in SNS Never reported for illegal action in SNS
A	Education : Jeil high school, Howon University, Address : Gunsan, Jeonrabuk-Do, Korea Hobby : Football, Inclination of politics : Progressive
	Groups in SNS : Football, Howon University Frequency of communication with User in SNS : about 10 times a day Frequency of communication with B in SNS : about 8 times a day
	Have no experience to ban others user or banned by other users in SNS Never reported for illegal action in SNS
B	Education : Gunsan high school, Howon University, Address : Gunsan, Jeonrabuk-Do, Korea Hobby : Football, Inclination of politics : Conservative
	Groups in SNS : Football, Howon University

	Frequency of communication with User in SNS : about 10 times a day Frequency of communication with A in SNS : about 8 times a day Frequency of communication with D in SNS : about 10 times a day
	Have no experience to ban others user or banned by other users in SNS Never reported for illegal action in SNS
C	Education : East Gunsan high school, Howon University , Address : Suwon, Korea Hobby : Baseball, Inclination of politics : Conservative
	Groups in SNS : Howon University Frequency of communication with A in SNS : about 2 times a day
	Banned twice in SNS Reported five times for illegal action in SNS
D	Education : Gunsan high school, Gwangju University, Address : Gwangju, Korea Hobby : Football, Inclination of politics : Progressive
	Groups in SNS : None Frequency of communication with B in SNS : about 10 times a day
	Have no experience to ban others user or banned by other users in SNS Never reported for illegal action in SNS

Table 5 divides users into categories by similarity. and Table 6 shows categories based on Table 5.

Table 6: Categories based on table 5.

Categories	Members
High School	Gunsan high school : User, B, D Jeil high school : A East Gunsan high school : C
University	Sungkyunkwan University : User, A, B, C Gwangju University : D
Inclination of politics	Progressive : User, A, D Conservative : B, C
Hobby	Football : User, A, B, D Baseball : C
Address	Suwon : User, A, B, C Gwangju : D
Groups in SNS	Football : User, A, B Sungkyunkwan University : User, A, B, C None : D

Now we can apply our proposed scheme to each user. Note that our proposed scheme computes the reliability of each user, and the reliability consists of two reliabilities: relationship and public. In this situation, we compute the reliability from the viewpoint of the User, not from A, B, C, or D. Our proposed scheme provides different values for each viewer, so the reliability may be different according to the viewer. Table 7 shows the reliabilities of entities A, B, and C from the viewpoint of the User.

Table 7: Font Sizes for Papers

Entity	Reliability				
	Relationship			Public	Total
	Parameter	Value	Total		
A	N	100	168	173	173
	V	50			
	F	18			
B	N	100	178	173	173
	V	50			
	F	28			
C	N	30	62	0	62
	V	30			
	F	2			

To show an example, we simplify our proposed scheme. All coefficients are set as 1, and each parameter is computed by simple summation, except N, which denotes the Degree of observance of norms. To compute N, we adopt subtraction from 100 based on each entity's illegal activities in the SNS. From the view of the User, there is no reliability for D, because there is no connection between the User and D, and our proposed scheme does not support this case.

CONCLUSIONS

SNSs have spread worldwide within a short period of time, because of their openness and convenience for sharing, and openness is considered a major characteristic and driving force of SNSs. But because accidents that violate personal privacy continuously occur due to that openness, maximizing the openness and minimizing the invasion of personal privacy still remains a real challenge.

The dynamic user reliability evaluation scheme suggested in this paper is for realizing the concept of reliability, which is in common use in our daily life, within the boundary of the SNSs as they are. The suggested scheme is able to be utilized as an index capable of evaluating the reliability of persons involved in an SNS, and it can be called a dynamic scheme, in that the value of reliability is not fixed, but varies by reflecting changes in relationship, as mutual reliability changes on a continual basis. The scheme is applicable to any kind of SNS, since it is possible to change functional elements of the suggested scheme, according to the type of SNS.

Because of the weighted value for the respective parameters, open reliability and relation reliability are configurable, depending on the user's individual inclination, so it can be utilized as a user-cantered evaluation scheme.

Accordingly, the suggested scheme is expected to be utilized as an index capable of evaluating another's reliability for protecting personal privacy, and controlling access in an SNS, by supporting a meaningful statistical analysis for the reliability of each node.

In addition, measuring the SNS users' reliability will make people try to observe norms, and communicate smoothly with each other, which will make a contribution, in making a green SNS environment, as a desirable service environment is established.

ACKNOWLEDGMENT

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No.R0126-15-1111, The Development of Risk-based Authentication·Access Control Platform and Compliance Technique for Cloud Security). First Author is Youngsook Lee and Corresponding Author is Younsung Choi (yschoi@howon.ac.kr)

REFERENCES

[1] Hanjae Jeong, Changbin Lee, Jin Kwak, Dongho Won, hangyoung Kwon and Seungjoo Kim, "Privacy-enhanced social network service (SNS)," The 2011 FTRA International Symposium on Advances in Cryptography, Security and Applications for Future Computing, 2011.

[2] Muthucumaru Maheswaran, Hong Cheong Tang, and Ahmad Ghunaim, "Towards a Gravity-Based Trust Model for Social Networking Systems," 27th International Conference on Distributed Computing Systems Workshops, 2007, pp. 24-31.

[3] Francis Fukuyama, Trust: The social virtues and the creation of prosperity, Free Press Paperbacks, 1230 Avenue of the Americas New York, 1996.

[4] Bimal Viswanath, Ansley Post, Krishna P. Gummadi and Alan Mislove, "An Analysis of Social Network-Based Sybil Defenses," Proceedings of the ACM SIGCOMM 2010 Conference, 2010, pp. 363-374.

[5] Anna Squicciarini, Federica Paci and Smitha Sundareswaran, "PriMa : An Effective Privacy Protection Mechanism for Social Networks," Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, 2010, pp. 320-323.

[6] Wei Wei, Fengyuan Xu, Chiu C. Tan and Qun Li, "SybilDefender: Defend Against Sybil Attacks in Large Social Networks," 2012 Proceedings IEEE INFOCOM, 2012, pp. 1951-1959.

[7] Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons and Abraham Flaxman, "SybilGuard: Defending Against Sybil Attacks via Social Networks," Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications, 2006, pp. 267-278.

[8] Sonja Buchegger, Doris Schioberg, Le-Hung Vu and Anwitaman Datta, "PeerSoN: P2P Social Networking: Early Experiences and Insights," Proceedings of the Second ACM EuroSys Workshop on Social Network Systems, 2009, pp. 46-52.

[9] Jeawook Jung, Hakhyun Kim, Jaesung You, Changbin Lee, Seungjoo Kim and Dongho Won, "Construction of a Privacy Preserving Mobile Social Networking Service," Proceedings of IT Convergence and Services, 2011, pp. 251-261.

[10] Weimin Luo, Jingbo Liu, Jing Liu and Chengyu Fan, "An Analysis of Security in Social Networks," 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009, pp. 648-651.

[11] Kim, Youngwoong, et al. "Dynamic Remote User Trust Evaluation Scheme for Social Network Service." Journal of the Korea Institute of Information Security and Cryptology 24.2 (2014): 373-384.

[12] Donghee Shin, "The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption," Interacting with Computers, vol. 22, no. 5, 2010, pp. 428-438.

[13] Lee, Changhoon, et al. "Dynamic user reliability evaluation scheme for social network service." Journal of the Korea Institute of Information Security and Cryptology 23.2 (2013): 157-168.

[14] Hanjae Jeong, "Hash-based Key Management Architectures for Social Networks Services," Ph.D. Thesis, Sungkyunkwan University, 2011.

[15] Maha Faisal and Asmaa Alsumait, "Social Network Privacy and Trust Concerns," Proceedings of the 13th International Conference on Information Integration and Web-based Applications and Services, 2011, pp. 416-419.