ABSTRACT

As interest in social network studies has grown bigger along with the development of the Web, social network trust management and applications have come into the spotlight. The increasing interest in social network services that are open systems has motivated the need for a reliable trust model that enables practical information sharing and information protection. In this paper, we propose an identity management-based social trust model for solving a sparsity problem and an information leakage. The proposed trust model contributes to increasing the opportunities for information sharing. In addition, the creation and use of identity groups with a clustering approach and partial identities in the proposed approach effectively address security and privacy risks in social networks. In experiments, the performance of the proposed approach is evaluated using precision–recall and $F$-measures. Copyright © 2011 John Wiley & Sons, Ltd.

KEYWORDS

social network; identity management; trust management; Web 2.0, Privacy

1. INTRODUCTION

Since the 1950s, many sociologists and psychologists have taken an interest in social networks in an attempt to analyze the social relationships between individuals or groups [1–3]. With the dramatic growth of the World Wide Web since the late 1990s, online communication has become a reality. The rapid increase of online activities and web information has led to rising interest in online social networks, which are open systems [4–6]. Online social networks generally refer to human networks that are formed through information sharing, exchanges, and transactions between users on the Internet. Although people in the real world make limited social relationships with friends, family, and colleagues, in the virtual world, people can make open social relationships with more diverse groups of people [7]. The psychological and social trustworthiness of people in traditional relationships could be recognized qualitatively based on past experience, but it is difficult to recognize relationships in online social networks based on qualitative background knowledge because of the diversity of those relationships. Therefore, it is important to analyze psychological and social information as electronic quantitative information in order to establish a trustworthy relationship model for online social networks [8].

User information, such as the behavioral activities and profiles of individuals that can be learned online, provide the basis for the quantification of social relationships [9]. Behavioral activity information refers to direct and indirect interactions between online users. Examples of this include the co-authoring of DataBase System and Logic Programming (DBLP) data sets [10] and the rating of the same contents in a rating system [7,11]. The social relationships between users can also be extracted through the agreement of content-based information. These types of relationships are formed under the assumption that users, whose shared information in profiles, and the like, agrees with one another, have similar tendencies [12]. Furthermore, the tendencies of a group composed of users with similar content-based information also have an indirect effect on the trusted relationships of the users [13–16].

Existing social trust models [12,17,18] focus on the quantification of relationships between users for reliable information sharing. They introduce the concept of FOAF (Friends Of A Friend) to realize the “maximum
sharing” in an information sharing system and infer the reliability of information obtained from extended relationships through a social trust model [19]. However, these existing social trust models can result in problems during the process of information sharing, such as information leakage and privacy. In other words, as unnecessary information access is permitted, regardless of the provider’s intent in the information sharing process, it becomes difficult to control the behavior of malicious users. Hence, in order to realize differentiated information sharing based on social networks, a privacy enhancement mechanism must be incorporated into the existing social trust models. Meanwhile, although existing trust-based information protection mechanisms manage information accessibility by the principle of “minimum privilege,” this process is not appropriate for open online social networks, and a new methodology is required [20,21]. What is needed is active identity management that can manage unique user identities because user identity, combined with behavior information, is not only the basis of information sharing but also a key to controlling information accessibility [22–26].

This paper proposes a reliable social trust model based on identity management for mediating information sharing and information protection in online social networks. For this purpose, the relationship model between users is quantified through the chronological records of users and the content-based extension of relationships. This will expand the information sharing opportunities by solving the sparsity problem in social networks. Furthermore, the proposed social trust model includes a mechanism for controlling access rights through active identity management. This plays the role of an information security guide by minimizing unnecessary information leakages in the course of information sharing. In order to understand the findings presented in this paper, readers are required to understand information protection-related terms that are not often used in conventional social network-based trust models for information sharing. Table I describes the important words that appear in this paper.

This paper is organized as follows. Section 2 introduces the related work. Section 3 discusses the entire architecture of the proposed model. Section 4 describes the social relationship extraction for constructing a social trust model. Section 5 discusses the identity group organizing process. Section 6 explains the relationship extension process with the identity group. In Section 7, the partial identity matching process is discussed. Section 8 defines the social trust model based on identity management. In Section 9, the experimental results are analyzed, and Section 10 is the conclusion.

### 2. RELATED WORK

Many studies on trust-based social networks have examined the quantitative relationships between users to effectively manage information systems. Ref. [27] inferred the trust between users by combining profile similarities and preferences on specific items. Ref. [12] proposed a method for combining the trust levels of users in a trust inference path on social networks and applied it to a recommendation system. Ref. [28] proposed a trust model that incorporates, in the existing trust model, the element of uncertainty that the user’s trust cannot be ascertained. These social trust models were applied both to email spam detection for filtering of unwanted information [29–31] and to recommendation systems for acquiring information in line with the users’ tendencies [17–19].

Meanwhile, maintenance and repair methods, using data mining techniques, were proposed to manage the relationship models of dynamic online social networks [32–34]. Furthermore, studies on predicting new links between users, which are expected to be formed in the future through existing links, attempted to improve the reliability of relationship models [35–37].

Even before online social networks came into existence, trust management has been used in information protection systems because they allowed effective management of information accessibility under uncertain situations. Ref. [38] introduced the concept of trust to the decision-making process in information access control for the first time. Since then, Ref. [39] proposed access control methods that incorporate the concept of trust in the user role and relationship structures. Many recent studies presented trust-based access control methods that are appropriate for various dynamic environments [40–42].

On the other hand, recent studies focus on the trust model based on user identity. Ref. [9] presented a methodology for creating a trust model, based on risk factors extracted from public key infrastructure and identity management, and using it as a certificate. Ref. [22] showed an access control method, based on identity management, which is suitable for the distributed Web service environment. This study addresses security problems that can occur in Web services by analyzing the identities of service providers that possess diverse characteristics. Ref. [43]

### Table I. Definitions of the notations.

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust</td>
<td>Expectancy of an agent to be able to rely on some other agent’s recommendations [50].</td>
</tr>
<tr>
<td>Identity</td>
<td>Any subset of attributes of an individual that uniquely characterizes this person within a community [51].</td>
</tr>
<tr>
<td>Partial identity</td>
<td>The characteristic of person in a specific context or role.</td>
</tr>
<tr>
<td>Identifiability</td>
<td>Property that an attribute must satisfy in order for decision to be possible [25].</td>
</tr>
<tr>
<td>Pseudonym</td>
<td>Identifiers of sets of subjects.</td>
</tr>
<tr>
<td>Role-relationship</td>
<td>Identifiers’ intersection of collaboration belongs to the same role.</td>
</tr>
<tr>
<td>pseudonym</td>
<td>One-time-use pseudonym for a transaction.</td>
</tr>
<tr>
<td>Transaction</td>
<td></td>
</tr>
<tr>
<td>pseudonym</td>
<td></td>
</tr>
</tbody>
</table>

expands the federated single sign-on system by expressing the goal of user-centric management in order to solve the privacy problem of the users who interact with a variety of services.

3. OVERVIEW OF THE PROPOSED ARCHITECTURE

This chapter gives an overview of the proposed architecture (Figure 1). The proposed system consists largely of four components: the Identity Group Generator (IGG), Social Relationship Extension Generator (SREG), Partial Identity Matching Generator (pIdMG), and Social Trust Generator (STG). The IGG assigns users’ identities to clusters based on their attributes, which are obtained from the user identity Database (DB). A user can have multiple identities and thus can belong to various identity groups. Clustering results are saved to the identity group DB. The SREG expands users’ relationships based on the user identity groups. The pIdMG performs partial identity matching to calculate the degree of correspondence between different users’ identities and determines the possibility of sharing information between users. The STG calculates a trust value to recommend users. The proposed system supports user identity management and the extension of user’s social relationships. As a result, it can support the information sharing of the next-generation Web, which is an open platform, and solve the problems of privacy and information protection that can be caused by the information sharing.

4. SOCIAL RELATIONSHIP EXTRACTION

In this section, structural properties originating from the interaction between users are used to extract social relationships. Social trust models can be divided into two types based on the types of relationships. The first deals with cases where relationships between users are one way (e.g., tagging in a blog, following in a twitter, sending or receiving e-mail messages). In these cases, although information flows in one direction, there are effects in the opposite direction; thus, the inverse operations of relationships should be considered [38]. The second deals with cases where relationships between users are two way (e.g., DBLP data set). In these cases, common links may be measured to define a trust model. In this paper, it is assumed that the relationship \( T_r \) between users is one way, and the trust model existing between users is determined by the degree of commonality maintained by the users (Figure 2, Equation (1)) [39]. Note that relationships extracted from the DBLP data set are, in fact, bidirectional. The measured trust value is normalized in the range of 0 to 10 using Equation (1). A trust value between users A and B, denoted by \( T_r(A, B) \), represents interaction frequencies between the users (i.e., \( E_{A,B} \)). In this case, if the trust score is zero, there is no relationship. Therefore, in the case of the DBLP data set used in this paper, the number of co-written publications becomes the trust score of relationships.

\[
T_r(A, B) = \frac{E_{A,B}(Interaction)}{E_A(Interaction)} \times 10 \quad (1)
\]

5. IDENTITY GROUP ORGANIZATION PROCESS

Attributes that characterize a user are extracted from the user’s profile to establish their identity. The extracted attributes are partitioned into \( k \) clusters using \( k \)-means clustering algorithms. A user’s identity in a social network service is a set of attributes that allocates the user to a group of similar users. In other words, a user’s identity is a set of identifiable attributes that distinguish that user (or
group) from others. In decentralized and dynamic social network systems, user profiles tend to have unspecified attributes. The clustering technique that is an unlabeled data classification scheme (one form of unsupervised learning) is suitable for categorizing user identities that encompass unlabeled data [24,25]. This paper makes use of publication information that is one of the attributes identifying users in the DBLP data set (the DBLP is composed of computer science bibliography data) [26]. Identity groups are formed by applying the $k$-means clustering algorithm [27] to the publication abstracts in the DBLP.

User attributes depicted in Figure 3 are used to form identity groups using clustering schemes. Each attribute denoted by $a_i$ consists of a set of terms as represented in Equation (2). The term frequency–inverse document frequency weight that is widely used to determine the relevance of a term in a given document is applied to the terms in the set.

$$a_i = \{t_1, t_2, t_3, \ldots, t_n\}$$

Equation (2)

The cosine similarity computation shown in Equation (3) is used to measure the relationship between attributes [48].

$$S_{ij} = \cos \theta = \frac{\vec{a_i} \cdot \vec{a_j}}{||\vec{a_i}|| ||\vec{a_j}||}$$

Equation (3)

To form identity groups, we applied $k$-means clustering to the similarity values of attributes measured using the equation above. For initialization, $k$ attributes are randomly chosen to form $k$ prototype clusters. The chosen attributes are representative of the members in each cluster. Attributes other than the representatives are allocated to a cluster (joined to a cluster as a member) in which the allocated attributes yield the highest similarity score with the cluster’s representative. When every attribute is allocated to a cluster, a new representative (attribute) for each $k$ cluster is selected for the newly formed clusters. To find an optimal cluster formation, we repeated the clustering process until no further changes are required in the formation of clusters, that is, the newly selected cluster representatives are the same as the previous ones (see Table II for the algorithm).

The formed identity groups are used in two ways. First, they are used to extend relationships between users in a social network by analyzing indirect interactions among
allows the discovery of identity settings such as isolated subgroups and isolated users. Also, in searches and recommendations using social networks, a phenomenon of remarkably decreased connectivity between users occur because of the shortage of source data. This paper proposes a way to extend relationships between users in a social network using identity groups (clusters of attributes). As shown in Equation (5), a user denoted by $U$ has a number of partial identities denoted by $id_n$.

$$U = \{id_1, id_2, id_3, \ldots, id_n\}$$

A partial identity consists of attributes that appear in both a set of user attributes and a set of the identity group attributes associated with the user (i.e., intersection is applied). The minimum number of attributes in a partial identity is one, and the maximum number of attributes that a partial identity can have is the total number of attributes associated with the user (Equation (6)).

$$id = \{attr_1, attr_2, attr_3, \ldots, attr_k\}$$

A user can have a partial identity that is also used as a partial identity for other users. The proposed trust model extends relationships between users through the partial identities shared by the users. The extension factor ($T_{EF}$) is computed with the number of identities in the identifiability set shared by the users (Equation (7)). The normalized range of the $T_{EF}$ value that is divided by the total number of identities of a user is 0 to 1.

$$T_{EF}(A, B) = \frac{\sum E_{A,B}(id)}{\sum E_A(id)}$$

The trust value associated with the relationship between users addressed in Section 4 is combined with the extension factor presented in this section to extend relationships in a social network. Originated trust value that comes from direct interaction has one or larger integer ranges as the quantity of overlapped common contents is measured. On the other hand, extension factor becomes to have positive decimals below one because they are measured with cosine similarity between users. As depicted in Figure 4, three different cases need to be considered in computing a trust value [46]:

(a) Interactions between the users occur but there is no relationship established via the extension factor.
(b) There is no interaction between the users, but a new relationship established via the extension factor exists.
(c) There are interactions between the users and relationships newly established via the extension factor.

In the case of (a), the trust value of an existing relationship measured using the equation in Section 4 is used as it is. In the other two cases where a new relationship is formed or the existing relationship is reinforced, a new equation is used. As shown in Equation (8), the trust value of the existing relationship and the extension factor are combined to produce the new value assigned to the extended relationship denoted as $T_r'$. For example, suppose that the trust value of an existing relationship built via direct interactions between user $A$ and $B$ is 3 and the extension factor is 0.5. The newly computed trust value with regard to the extended relationship is 3.5.

$$T_r(A, B) = T_r(A, B) + T_{EF}(A, B)$$

The range of the trust value computed using the equation above is between 0 and 11, so Equation (9) is used to normalize the trust value in the range of 0 to 10.
We propose a new alternative for computing trust scores that decomposes direct and indirect relationships between users. In the case of a direct relationship, the three types are adjusted to a trust score ($T_{Sr}$).

$$T_{Sr} = \begin{cases} T^r & \text{if relation is direct relation} \\ T^i \times 10 & \text{indirect relation} \end{cases}$$

In the case of direct relationships, we can simply use the primary value. For extracting the trust score of an indirect relation, we need to synthesize the various types of relationship, however, because they have the differential ranges of value. The trust score of an indirect relationship ($T^i$) is accordingly normalized using Equation (11). Figure 5 shows this normalization method. There is an indirect relationship composed of two actual relationships. The inferred trust score of this indirect relationship is 25. (However, we do not have to consider the calculation that has several duplicate paths.)

$$T^i = \frac{\prod T_{Sr}}{10^{k-1}}$$

Newly established relationships provided by the proposed relationship extension approach allow more opportunities for information sharing that support the collective intelligence of Web 2.0. To minimize side effects in the relationship inference approach that combines direct connections with indirect connections in a social network, the proposed approach exploits the relationship extension factor that influences the calculated trust value.

7. PARTIAL IDENTITY MATCHING FOR IDENTITY MANAGEMENT

This section presents the group-aware identity management approach that manages the user identities in a social network. In online social networks, people are connected to each other in various ways (i.e., there are various types of relationships). Because a user is associated with many different attributes, it is relatively easy to create and use an identity that reflects personal preferences and interests. In addition, creating and using different identities are generally easier in the online world. However, a more complex personality can be assigned to users because they participate in many different relationships. In addition, user access control is necessary for security in social network systems. Individuals in a system should be identified, and access to the resources in that system should be controlled by placing restrictions on the established identities [11]. That is, identity management is required.
to prevent privacy violations and data leakage caused by unauthorized access.

The proposed group-aware identity management approach combines relationship-based identity and role-based identity to manage user identity (Figure 6). The relationship-based identity is derived from the trust value of direct or indirect relationships between users described in the previous section. The trust value that considers historical interactions between users can represent vulnerability and a positive expectation residing in the relationship. In role-based identity, user identity is analyzed to determine their role in various social interactions (student and teacher in a school, player and coach in a basketball team, etc). To effectively manage a user identity that has diverse characteristics, the user attributes are formed into a set of partial identities. Each user has diverse identities that signify his role in various fields. A partial identity is defined as the specific characteristic of users. As shown in Equation (12), the user’s personality ($P_i$) is represented as the sum of partial identities.

$$P_i = \{\text{pid}_1, \text{pid}_2, \text{pid}_3, \ldots, \text{pid}_k\} \quad (12)$$

As mentioned earlier, identity groups are used to determine the identifiability of the anonymity set. Along with the use of pseudonyms that represent the roles associated with the user, the user identity consists of many partial identities, each of which represent the user in a different context. When another user (a requester) requests access to a user’s information (resources), the resource owner verifies the partial identities of the requesting peer that are identical to their own partial identities (Equation (13)).

$$C_i(A, B, \text{pid}) = E_{A, \text{pid}, B, \text{pid}}(\text{attr}) \quad (13)$$

If the verified partial identity satisfies the condition for authorizing access, denoted by $c$, the resource owner gives a positive value (+1) to the requesting peer’s role-based identity denoted by $IdM_{role}$. Otherwise, a negative value ($-1$) is given, as shown in Equation (14).

$$IdM_{role}(A, B, \text{pid}) = \begin{cases} +1 & C_i(A, B, \text{pid}) \geq c \\ -1 & \text{otherwise} \end{cases} \quad (14)$$

8. IDENTITY MANAGEMENT-BASED SOCIAL TRUST MODEL

This chapter presents a social trust model that combines the social relationship information with an identity-based factor. This model incorporates an information protection mechanism in the trust model to address information leakage and privacy problems during the information sharing process. Access level is determined by identity matching, and according to the result, access to information that is not appropriate for the user can be controlled. The final value of the social relation model ($T_{idM}$) is expressed as a multiplication of the role identity matching value ($IdM_{role}$) and the trust value ($TS_r$) of the relationship between the users.

$$T_{idM}(A, B) = IdM_{role}(A, B) \times TS_r(A, B) \quad (15)$$

In general, trust levels are divided into five steps, according to access level, as shown in Table III [47,48]. The proposed method does not consider the handling method for level 1 in the five levels of accessibility for permission. This is because DBLP data set is based on specific interactions between users. Level 0 is assigned the role identity value of $-1$ and expresses the case of distrust in which the information requester is not appropriate for the accessed resource. In this case, the information accessed by the user is blocked to prevent unwanted information leakage. Level 2, which is minimal permission, expresses the concept that even if the requester did not have direct or indirect interactions, he or she is an appropriate user for the nature of the resource. In this case, access can be determined by the information provider’s request. Trust level 3 expresses free access to information, except when the information provider wants minimum sharing of the information. This means that relatively free access by the information requester is allowed, including direct and indirect interactions, and that the user is appropriate for the nature of the resource. Level 4, in particular,

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 0</td>
<td>Distrust</td>
<td>Completely untrustworthy</td>
</tr>
<tr>
<td>Level 1</td>
<td>Ignorance</td>
<td>Cannot decide</td>
</tr>
<tr>
<td>Level 2</td>
<td>Minimal</td>
<td>Lowest trust</td>
</tr>
<tr>
<td>Level 3</td>
<td>Average</td>
<td>Mean trustworthiness</td>
</tr>
<tr>
<td>Level 4</td>
<td>Good</td>
<td>Trusted by major population</td>
</tr>
<tr>
<td>Level 5</td>
<td>Fully trust</td>
<td>Fully trustworthy</td>
</tr>
</tbody>
</table>

Figure 6. A process for the user identity management.
defines the access by information requesters who have a social trust value of 9, or higher, which corresponds to the top 10% in the trust index. Information requesters who belong to this group can access all public information.

Figure 7 shows the general relationship between the user’s information accessibility and the importance of the information. Accordingly, as the importance of the information increases, the cases of denied access increase and the number of users who can interact with the transactions decreases. Because of the sparsity problem of social relationships, social networks more distinctly demonstrate this hierarchical structure. Thus, the relationship model between information requester and information provider is useful for minimizing information leakage and controlling anonymous information access. For this purpose, users set credential values in the information sharing process to open their information only to users who meet the prescribed conditions. In this paper, access is denied for level 0 information only, assuming that the information provider’s credential values are set to the minimum. This is because this paper combined the concepts of information protection based on the social Web principle of “maximum sharing.”

9. EXPERIMENTS

9.1. Experimental set-up

In this paper, experiments are conducted based on the DBLP [10] distributed in June 2009. We implement a prototype of the recommendation system for these experiments. In order to construct social network with DBLP data set, we collect 470 users and follow 674 publication lists (Table IV). The number of direct relationships between the users is about 1500. In addition, we supplement the abstracts of publications to the user attribute to improve the user identity analysis. To conduct the experiments, we extracted two types of information: (i) relations between the individuals with co-author information and (ii) attributes of the node, which is the abstract of publications. The first information, which represents a set of social relationships, made the actual relations. The second information is used to organize the identity groups with clustering approach. Clusters are organized with similarity between the attribute of users.

The experiments are separated to analyze the identity group optimization and the performance evaluation of the proposed approach with precision–recall and F-measure.

9.2. Experimental result

Figure 8 shows the cluster evaluation factor in each number of clusters. In this proposed approach, the k-means clustering approach is applied to organize the identity group with unlabeled data. The number of clusters affects the optimization of the identity groups. The cluster evaluation factor is derived from the summation of the similarity values among all identities in and the deviation values in each identity group. The optimized identity groups have much higher similarity value and much lower deviation value. It means that cluster evaluation factor (Eval_cluster) is proportional to the similarity value but inversely proportional to the deviation value (Equation (16)). This graph shows that the optimum number of identity groups is around 15–18 for this data set. For the rest of the experiments, we set k to 16.

\[
Eval_{\text{cluster}} = \frac{\sum \text{Sim}(A, B)}{\sum \text{dev}(A, B)}
\] (16)

F-measure is used to measure the performance of the proposed approach. Precision and recall are standard measures for exactness and completeness, respectively [49]. F-measure ($F_1$) is the harmonic mean of precision and recall. Among others, $F_1$ measure in which recall and precision are evenly weighted is selected.

### Table IV. A specification of data set extracted from DBLP for this experiment.

<table>
<thead>
<tr>
<th>Data set</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A number of authors</td>
<td>459</td>
</tr>
<tr>
<td>A number of publications</td>
<td>665</td>
</tr>
<tr>
<td>A number of direct relationship</td>
<td>1479</td>
</tr>
<tr>
<td>An average number of papers per author</td>
<td>2385</td>
</tr>
</tbody>
</table>
The performance of the proposed approach is summarized in Figure 9. The experimental result is compared with the filtering method and relationship extension method in terms of the precision–recall and F-measure. We extract the top-k recommendation results in each method. In this experiment, we set k to 20. The proposed approach improves the precision and recall by 30%, and 23% as compared with the filtering method. It also shows that the F-measure of the proposed approach is increased by 27%, and 13% as compared with other methods, respectively. The suggested approach’s precision and reproduction rates are a lot higher than those of the previous methods. The improved reproduction rate reflects the varied recommendations by expanding the users’ limited relationship model. It means that the proposed approach has a better outcome for the sparsity problem. In addition, the precision rate has improved by obtaining results based on the reliability model, which reflects the users’ identities from various recommendation clusters. The existing filtering method and relationship extension method focus on improving either the precision or reproduction rate, but not both. The suggested method, however, improves both of these factors, thereby improving the reliability of the synthetic recommendation results shown by the F-measure. It means that the proposed trust model contributes to increasing the opportunities for information sharing.

### 9.3. Analysis and discussion

To evaluate the excellence of the proposed method, this experiment built a social network based on DBLP data sets and evaluated the value of shared information during the course of information sharing between the users through the precision–recall and F-measure indices. The results showed that the proposed social trust model could be used...
to maximize information sharing on the social web. In this process, a trust relationship model, based on user identity, was used to present the starting point for solving the information leakage problem, which is a weakness of the social web. Because this paper focuses on maximum sharing and reliability of information on the social Web, applying evaluation indices for information protection is insufficient. Furthermore, detailed analyses about information leakage and privacy issues, and their harmonization with the existing social network-based technologies, needs to be examined continuously.

10. CONCLUSIONS

As the interest in social network studies has grown bigger along with the development of the Web, social network trust management and applications have come into the spotlight. In this paper, we propose an identity management-based social trust model for solving a sparsity problem and an information leakage. The proposed approach was described as a potential solution for providing a reliable social network services. We aim to provide an information sharing and a privacy enhancement. In a social network, not only the relationship extension method solves the sparsity problem but also the partial identity matching method realizes the reliable transactions guaranteeing the privacy enhancement.

The proposed approach can be extended in a context-aware social network. To seize the dynamic user propensities, cognitive social network approaches should be accompanied with proposed social trust model. Furthermore, identity management-based social trust model can be applied to the real world applications such as recommendation system and E-mail spam detection.

ACKNOWLEDGEMENT

Project supported by the Chung-Ang University Research Scholarship Grants, Korea.

REFERENCES


44. Murata T, Moriyasu S. Link prediction of social networks based on weighted proximity measures, presented at the IEEE/WIC/ACM International Conference on Web Intelligence, 2007.


47. Li HH, Singhal M. Trust management in distributed systems. Computer Feb 2007, 40; 45.


