Cluster Comput
DOI 10.1007/s10586-013-0248-9

# Trust management on user behavioral patterns for a mobile cloud computing

**Mucheol Kim · Sang Oh Park**

Received: 23 January 2013 / Accepted: 27 February 2013


**Abstract** With the development of ubiquitous computing technology, users are using mobile devices which are for producing and accessing information. Due to the limited computing capability and storage, however, mobile cloud computing technology are emerging research issues in the architecture, design, and implementation. This paper proposes the trust management approach by analyzing user behavioral patterns for reliable mobile cloud computing. For this, we suggest a method to quantify a one-dimensional trusting relation based on the analysis of telephone call data from mobile devices. After that, we integrate inter-user trust relationship in mobile cloud environment. As a result, trustworthiness of data in data production, management, overall application, is enhanced.

**Keywords** Mobile cloud computing · Social networks · Trust management · Information technology

## 1 Introduction

Cloud Computing is a method in which users access various computing resources and computing power of their own in a network environment [1–3]. Tasks are performed efficiently and economically via outside infrastructure. It could realize that the users can access the data wherever and whenever they want [4]. Cloud computing technology is transferred from previous distributed computing technology such as grid computing and utility computing [8] (Fig. 1). The cloud computing service has been incorporated in various areas as the technology of virtualization and network environment have become sophisticated. Not only that, as the web technology has evolved to collective intelligence, cloud computing has been lauded as one that suits the needs of the web 2.0 paradigm [5, 6].

In addition, mobile devices such as smartphones and tablets have become sophisticated enough to replace conventional computing devices that they are currently accepted as an important part of everyday life [7]. Users are now able to acquire and produce various kinds of information and data using diverse mobile applications and the web in wireless network environment wherever and whenever they want. This has led to production of more information, yet the storage and computing solutions have not developed in tandem, which calls for adoption of mobile computing [9]. Mobile clients share their roles within their cloud via outsourcing, thereby increasing the overall efficiency of the process being carried out.

Establishing a cloud environment with resources in smartphones is a representative case of mobile cloud computing [10]. Each mobile device performs its own role and the outputs are collected into the cloud. This environment allows for resource sharing and distribution of computing load [11]. Data collected with user experience is also possible, thus a tool to measure trustworthiness of data is offered. Compared to a system in which only a select few produce and share data, cloud computing environment explosively increases not only the amount but also the complexity of data. Therefore, the following themes have become ever

M. Kim
NTIS Center, Korea Institute of Science and Technology Information, 245 Daehak-ro, Yuseong-gu, Daejeon, Korea
e-mail: mucheol.kim@gmail.com

S.O. Park (✉)
Department of Global Scientific Data Hub, Supercomputing Center, Korea Institute of Science and Technology Information, 245 Daehak-ro, Yuseong-gu, Daejeon, Korea
e-mail: sopark3@gmail.com

Published online: 10 April 2013

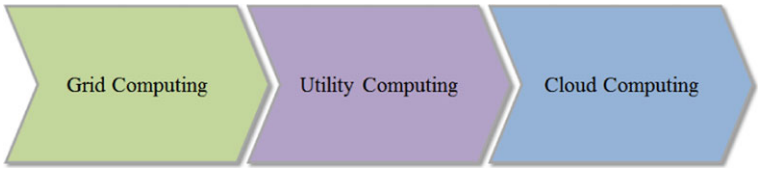


**Fig. 1** The trends of IT services environments

more important under distributed computing environment: efficient data collection and data integration, management, and flow of trustworthy data [12]. Specifically, production and flow of trustworthy data goes beyond the effect of mechanical resource sharing, and pursues flexibility and scalability that mobile cloud computing technology aims at by realizing heuristic and intelligent resource management and efficient distribution of computational performance.

It is important to analyze relationship to offer user-customized data. Thus it has become necessary to analyze the trustworthiness of the relationship between the data sources in order to manage and take advantage of data in cloud computing environment. This paper proposes a global social trust model building system by seamlessly integrating the one-dimensional trust relation values. This paper analyzes interactions between users in mobile computing environment. For this, we suggest a method to quantify a one-dimensional trusting relation based on the analysis of telephone call data from mobile devices. Quantified social trust model supports inter-user trust relationship and integration. In other words, the proposed approach not only helps decide channeling path of trustworthy data in cloud environment but also helps address security issues with increased trustworthiness of data because our approach enlarges trusting relations between users with the concept of FOAF (Friend Of A Friend). By doing so, a channeling path for trustworthy data under cloud environment is suggested. With enhanced trustworthiness, the issue of security also can be addressed. As a result, trustworthiness, that is, accuracy and timeliness of data in data production, management, overall application, is enhanced.

In Sect. 2, related works are described. Section 3 explains our trust management approach to build a mobile cloud. Section 4 has its implementation and the result. Section 5 discusses some research issues from the proposed approach. Finally in Sect. 6, the suggested method is summarized and ideas for further study are suggested.

## 2 Related works

Cloud computing is a model for enabling convenient, on-demand network access to shared resource (e.g., networks, storage, applications and services). There are a number of commercial cloud providers such as Amazon EC2 [13] and S3 [14], Google App Engine [15], Microsoft Windows Azure [16] and so on.

Interest in analysis and utilization of data obtained from smartphones has increased as smartphones have spread widely.

Previously, the social network-based cloud integration has been explored cloud platform in order to host social networks, or it has been using social networks to extend the application. For example, amount of users of social network services can make scalable cloud based applications with provided open API such as Amazon Web Services, OpenSocial [17] etc. PolarGrid [18] extracts social data with OpenSocial and OpenID [19].

The structure of a social network is essentially a dynamic virtual group with trust relationships between users. Many studies have attempted to define relationships with social trust models [20–22]. Reference [21] proposed a trust model that is appropriate for online communities using the user profiles. [22] suggested a trust model that reflects the element of uncertainty users' information. Meanwhile, various studies analyze and mine social networks that are expressed as relational networks [23, 24]. Reference[25] proposed the provisioning and management approach based on collaborative strategy with social relationships in cloud computing services.

Interest in analysis and utilization of data obtained from smartphones has increased as smartphones have spread widely. [26] proposed a method to filter out voice spam calls on the IP telephony system that recognizes relationships between users by analyzing sustained phone-calling behavioral pattern (i.e. duration, frequency, recent history etc.) extracted from smartphone call log. [27] built a social network by analyzing a phone call log. [28] studied the contact lists and phone call histories of smartphone users and extracted the behavioral pattern of each user, by built a social network. It can produce a recommended user list for a user when making a decision; it also suggests a standard to address privacy issues that occur in data sharing.

## 3 Trust management on user behavioral patterns for a mobile cloud computing

In this chapter, we propose a trust management approach on user behavioral patterns for a reliable mobile cloud computing (Fig. 2). Users establish their own social network led by themselves. For example, they live in diverse relationships

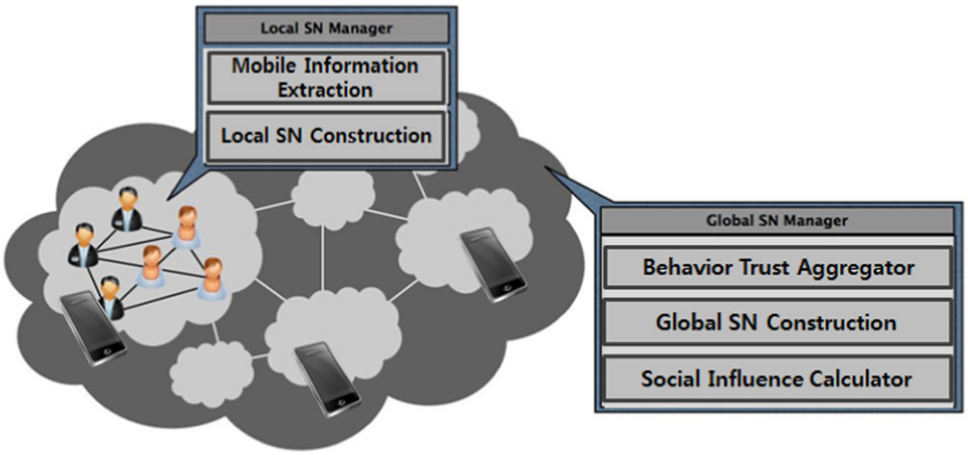


**Fig. 2** Overview of the proposed trust management framework in mobile cloud environment

such as explicit relationships such as friends in a school, colleagues at work and family members and implicit relationships in which they share common interests such as hobby and duties. In our approach, the social relationship between users in mobile cloud environments is inferred by behavioral patterns in mobile phones. This kind of social network with one-dimensional perspective is called 'local social network.' However, it is not easy to facilitate the expansion of information using the social network in explicit or implicit relationship on the first stage. Therefore, it is very important to establish a global social network using each user's local social network in the process of inferring information using social network integrations.

Meanwhile, reliability on the inferred information in indirect connections, which are composed of several direct link paths, is a critical issue in the expansion of information. Hence, it is also important to establish a social network by investigating and quantifying social influence among users in the process of establishing local social networks to assess and infer the reliability of information. In this chapter, therefore, call log was extracted from smartphones, and whether or not inter-user relationships were formed was examined based on the extracted personal information. Then, quantitative values were extracted and expressed as abstractive trust values. In terms of behavioral pattern determinants, the formation and degree of inter-user relationships can be analyzed through analysis on users' interactions (i.e. collaborative relationship in academic activities), phone calls and SMS. To enhance the reliability of inter-user relationship, users' behavioral patterns in mobile environment have been analyzed and quantified into trust values. Then, a behavioral determinant based social trust model has been established.

Trust values are quantified and abstracted based on the details of smartphone calls to find out users' behavioral pattern determinants (Fig. 3). A call log handled in this chapter refers to interactions with direct relations such as family, colleagues and friends. Therefore, users' relationships

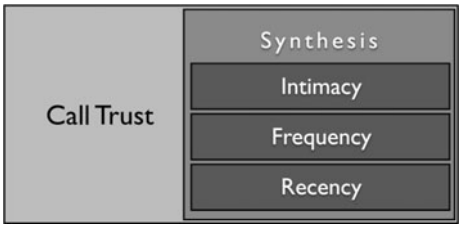


**Fig. 3** Behavioral trust model in a smartphone

are quantified by analyzing call patterns based on call frequency, intimacy (or duration) and recency among users. In this study, local social networks which represent each user's direct connections were built by analyzing inter-user call behaviors in the following three aspects; frequency, intimacy and recency.

First, inter-user relationships are defined through call frequency ($Frequency_{A,B}$) among users [Eq. (1)]. Call frequency from smartphones represents the level of connections among the users. In this study, call frequency is defined as 'total number of calls among users.' In other words, if the call frequency between 'User A' and 'User B' is greater than that between 'User A' and 'User C,' it is understood that 'User A' trusts 'User C' more than 'User B.' In other words, a user may trust his friend to whom he talks on the phone every day more than his colleagues at work to whom he talks on the phone for a significant time but with less frequency.

$$Frequency_{A,B} = \frac{Talk_{A,B}}{\sum_{k=1}^{n} Talk_{A,k}} \tag{1}$$

As shown in Eq. (1) above, the trust value between 'User A' and 'User B' is calculated with the call frequency ($Talk_{A,B}$) between 'User A' and 'User B' against the frequency of calls ($\sum Talk_{A,B}$) that 'User A' called to all other users ($N$ users).

$$Intimacy_{A,B} = \theta \cdot DurationS_{A,B} + (1-\theta) \cdot DurationR_{B,A} \tag{2}$$

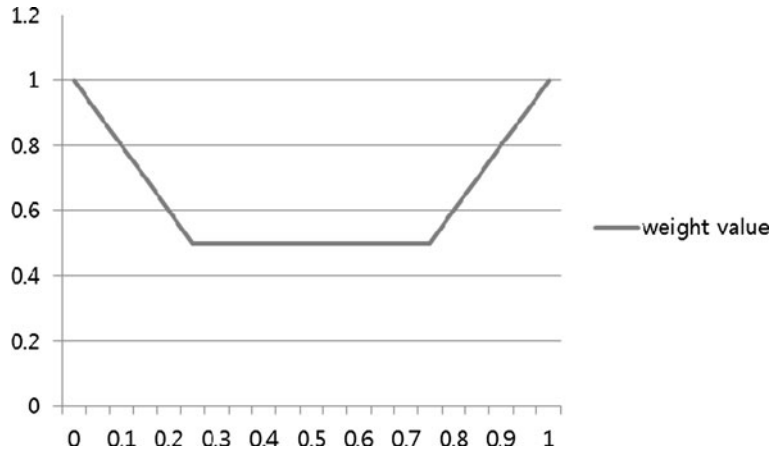


**Fig. 4** Flow of the weight value followed ratio of tendency

Equation (2) above calculates intimacy ($Intimacy_{A,B}$) between 'User A' and 'User B." Intimacy refers to the duration of inter-user relationship. In other words, if the duration of relationship is low despite high frequency in formation of relationship, the assessment on the frequency should be readjusted (i.e. system robustness on the formation of malicious relationship might be provided to enhance trust values). On the contrary, high intimacy despite low frequency in formation of relationship means that inter-user reliability should be reassessed to a higher level. In this study, intimacy has been defined the duration of calls among users. In other words, the fact that the call duration between 'User A' and 'User B' is longer than that between 'User A' and 'User C' means a possibility of high intimacy and high reliability. In this study, weighted value ($\theta$: the weighted value of the send) is applied after dividing duration-based intimacy into post-send duration ($DurationS_{A,B}$) and post-reception duration ($DurationR_{A,B}$) to reflect smartphone users' diverse call patterns such as those who usually use the send function or those who use the reception function only.

$$DurationS_{A,B} = \frac{\sum D_{A,B}}{\sum_{k=1}^{n} D_{A,k} + \sum_{k=1}^{n} D_{k,A}} \tag{3}$$

Send duration ($DurationS_{A,B}$) can be obtained through total call duration ($\sum D_{A,B}$) between 'User A' and 'User B' against the total call duration ($\sum_{k=1}^{n} D_{A,k} + \sum_{k=1}^{n} D_{k,A}$) that 'User A' had with all other users ('n' users in total) in the Eq. (3).

$$DurationR_{A,B} = \frac{\sum D_{B,A}}{\sum_{k=1}^{n} D_{A,k} + \sum_{k=1}^{n} D_{k,A}} \tag{4}$$

On the contrary, call-reception duration ($DurationR_{A,B}$) refers to time taken after 'User B' sends to 'User A' as shown in the Eq. (4).

$$Tendency_A = \frac{\sum_{k=1}^{n} D_{A,k}}{\sum_{k=1}^{n} D_{A,k} + \sum_{k=1}^{n} D_{k,A}} \tag{5}$$

In this study, users' call tendency is analyzed to calculate the weighted value of the send and reception. In Eq. (5), the percentage of duration caused by users' call or reception is calculated. The send percentage ($Tendency_A$) refers to total call duration that 'User A' spent to send against the total send or reception duration (a reception ratio is calculated with $1 - Tendency_A$.).

$$\begin{cases} Tendency_A < 0.25 & \rho = -2 \cdot Tendency_A + 1 \\ 0.25 \le Tendency_A \le 0.75 & \rho = 0.5 \\ Tendency_A > 0.75 & \rho = 2 \cdot Tendency_A - 1 \end{cases} \tag{6}$$

The calculated send ratio ($Tendency_A$) determines the weighted value ($\rho$) depending on its scope as shown in Eq. (6). If call tendency is 'send-centered (i.e. 0.75 or higher of send ratio), it is divided into 'reception-oriented (i.e. 0.25 or lower of reception ratio)' and common case (Fig. 4).

Lastly, recency ($Recency_{A,B}$) refers to the time flow of relationship among users using the recent call log. In other words, yesterday's call is more trustable than the call a month ago, which is the result obtained after reflecting the uncertainty of diverse changes over time on trust values among users. In other words, inter-user reliability continues to decline over time due to increase in uncertainty.

$$Recency_{A,B} = \frac{N - Rank_{A,B}}{N} \tag{7}$$

In Eq. (7), it is expressed as call recency ($Rank_{A,B}$) among users against total records ($N$ users) in the recent list of call records in which redundant calls are removed. In other words, the weighted value of trust on recency is added to those who made the recent call records. Lastly, users' customary behaviors information which can be extracted from the call log can be obtained through synthesis of frequency, intimacy and recency. The synthesis of these three factors ranges from '0' to '1' in real number [Eq. (8)]. It is performed for generalization with customary behavior information which can be acquired from different information.

$$\begin{aligned} T_{BD} = {} & \alpha \cdot Frequency_{A,B} + \beta \cdot Intimacy_{A,B} \\ & + \chi \cdot Recency_{A,B} \\ & (\alpha + \beta + \chi = 1,\ 0 \le \alpha, \beta, \chi \le 1) \end{aligned} \tag{8}$$

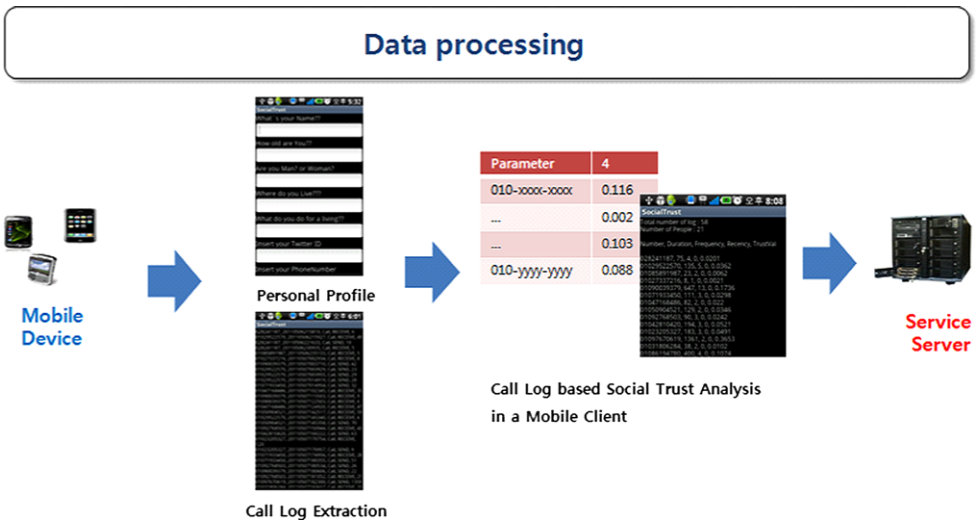


**Fig. 5** Extraction of call records and personal information from smartphone

**Table 1** Summary of information for implementation of social network in mobile environment

| Summary of Smartphone Environment Information for Development | |
|---|---|
| No. of Users | 804 |
| Call Log | 18202 Calls |
| No. Average Calls per User | 22.6 Calls/Person |

## 4 Implementations and analysis

In this section, the implementation and service scenario of the framework on autonomic cognitive social network is explained. In fact, it is built based on users' call log and personal information in smartphone environment. As shown in Sect. 3, the implementation process is as follows; construction of local social network in client, collection in the server and construction of global social network.

In this study, samples were extracted, and a test was performed as shown in Table 1 to acquire necessary information from smartphones such as users' customary behavior information, personal information and details on SNS activities. Smartphone call records were extracted against Android smartphones (Android Froyo 2.2). A total of 18,202 calls (approximately, 23 calls per user) were extracted from 804 users. The extracted call records were used in establishing each user's personal local social network as customary behavior information among users. Because they include users' personal information such as gender, age, occupation and address, they can be used as personal information determinants.

First, to build a social network, users' call records were extracted in smartphone (especially Android) environment, and applications which get personal information were developed. The extracted call records are used to build a local social network which reflects call frequency, intimacy


**Fig. 6** Call log-based trust value in a mobile client

and recency that were stated in Sect. 3. Then, the local social network and personal information are sent to the server (Fig. 6). The inter-user relationship on a local social network is abstracted and quantified into trust value as shown in Fig. 5. Inter-user trust values range from '0 (not related)' to '1 (closely related).' The results are used in establishing local social networks which express connectivity and relationship levels among users in direct relations.

Figure 7 reveals a process of developing a global social network based on customary behavior information. Each local social network built from the client is sent to the server along with the input information from the personal information input application. In the server, a global social network is built by integrating local social networks which were created through call log, one of users' customary behavior information. Then, the global social network is sent to users through each client.

Figure 8 reveals trust values between users on a global social network which are constructed with the explained process in Fig. 7. Users' direct relations which come from call logs have higher trust values, and new relations are being formed through indirect relations from FOAF inferences. Based on users' customary behaviors, high-ranked users'

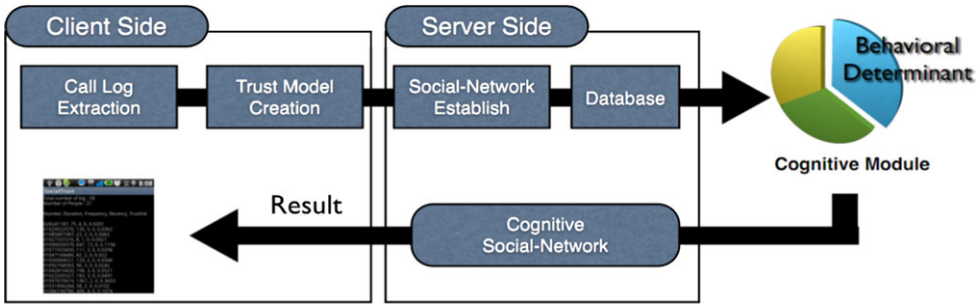


**Fig. 7** Process of customary behavior information-based social networks

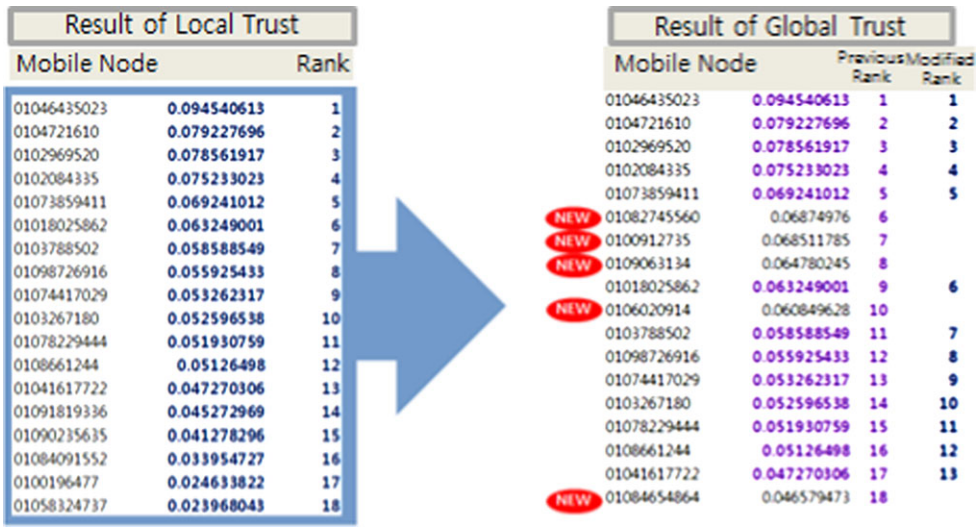


**Fig. 8** Proposed integrated global social trust model

rank displays pretty similar results. In terms of the relation with a newly added friend, it is the FOAF inferences with high trust value among the friend log with high trust value. In other words, we could infer trustworthy relationships with multi-paths (or indirect relationships) which might consist of reliable individuals in a mobile cloud environment. Furthermore, reliable individuals should have amount of obvious contacts or similar behavioral patterns of mine.

## 5 Key research issues

Some of the major challenges of mobile cloud computing research include both reliability and security concerns. The introduction of the proposed approach brings new research in these research fields. The reliability of mobile cloud computing involves providing quality of data with evaluated relationships in mobile cloud environments. The relationships represent trustworthiness of each mobile client. The challenge here will be to proceed to appropriate reliable data (or resources) distribution mechanisms and integration processes in mobile cloud environments. Furthermore, the proposed trust management can be applied to the incentive mechanism for reliable discovery and selection of the resources.

On the other hands, mobile cloud computing technology gives rise to security problems, such as privacy and data leakage. In other words, as unnecessary data access is permitted, regardless of the distinct intent in the data sharing process, it becomes difficult to control malicious access. The proposed trust management could induce to new approaches for resolving security problems related to identity of mobile clients. An identity is a representation of an entity in a specific application domain [29]. What is needed is identity management that can control unique identities of mobile clients with behavior information is a key issue to preventing unpermitted access and data leakage.

## 6 Conclusions

With the advancement of communication environment and web technology, more people started to express their opinions and share information with mobile devices. However, there are distinct limitations such as restricted computing capability and lacking storages. Thus, mobile cloud computing is emerging research issues in information technology. This paper proposes the trust management approach for reliable data integration, management and applications in

mobile cloud computing environments. To provide trustworthy information, this study has attempted to analyze interactions among users in mobile environment. For this, it has built one-dimensional trust and proposed a way to quantify it by analyzing information on phone calls of mobile devices. In addition, trust-based mobile cloud has been constructed by integrating mobile client information. In future studies, we should extend in context-aware approaches with social information in mobile cloud computing environments. We should also analysis social influence models with personal determinant (i.e. similarity of user profiles etc.) and environmental determinant (i.e. user activity based community detections etc.) in a mobile cloud environment.

## References


1. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M.: A view of cloud computing. Commun. ACM **53**(4), 50–58 (2010)
2. Zhang, Q., Cheng, L., Boutaba, R.: Cloud computing: state-of-the-art and research challenges. J. Internet Serv. Appl. **1**(1), 7–18 (2010)
3. Katsaros, D., Mehra, P., Pallis, G., Vakali, A.: Cloud computing: distributed Internet computing for IT and scientific research. IEEE Internet Comput. **13**(5), 10–13 (2009)
4. Gnanasekar, J.M., Ponmagal, R.S., Anbalagan, P.: In: Integration of Wireless Sensor Network with Cloud, International Conference on Recent Trends in Information, Telecommunication and Computing, pp. 321–323 (2010)
5. Bubendorfer, K., Caton, S., Rana, O.F.: Social cloud computing: a vision for socially motivated resource sharing. IEEE Trans. Serv. Comput. **5**(4), 551–563 (2012)
6. Pallis, G.: Cloud computing: the new frontier of Internet computing. IEEE Internet Comput. **14**(5), 70–73 (2010)
7. Dinh, H.T., Lee, C., Niyato, D., Wang, P.: A survey of mobile cloud computing: architecture, applications and approaches. Wirel. Commun. Mob. Comput. Published Online (2011). doi:10.1002/wcm.1203
8. Yeo, S., Venugopal, S., Chu, X., Buyya, R.: Autonomic metered pricing for a utility computing service. Future Gener. Comput. Syst. **26**, 1368–1380 (2010)
9. Heurta-Canepa, G., Lee, D.: A virtual cloud computing provider for mobile devices. In: Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services, p. 6 (2010)
10. Christensen, J.H.: Using RESTful web-services and cloud computing to create next generation mobile applications. In: Proceedings of the 24th ACM SIGPLAN Conference Companion on Object Oriented Programming Systems Languages and Applications, pp. 627–634 (2009)
11. Rimal, B.P.: A taxonomy and survey of Cloud computing systems. In: Fifth International Joint Conference on INC, IMS and IDC, pp. 44–51 (2009)
12. Takabi, H.: Security and privacy challenges in cloud computing environments. IEEE Secur. Priv. **8**(6), 24–31 (2010)
13. Amazon, W.: Services EC2. http://aws.amazon.com/ec2/
14. Amazon Simple Storage Service(Amazon S3), http://aws.amazon.com/s3/
15. Google App Engine: https://developers.google.com/appengine/
16. Microsoft Azure: http://www.windowsazure.com
17. OpenSocial: http://www.opensocial.org/
18. PolarGrid: http://www.polargrid.org/
19. OpenID: http://openid.net/
20. Kim, M., Seo, J., Noh, S., Han, S.: Identity management-based social trust model for mediating information sharing and privacy enhancement. Secur. Commun. Netw. **5**(8), 887–897 (2012)
21. Kim, M., Park, S.: Group affinity based social trust model for an intelligent movie recommender system. Multimed. Tools Appl. **64**(2), 505–516 (2013)
22. Kim, S., Han, S.: The method of inferring trust in web-based social network using fuzzy logic. In: International Workshop on Machine Intelligence Research (2009)
23. Barabasi, A.L., Jeong, H., Neda, Z., Ravasz, E., Schubert, A., Vicsek, T.: Evolution of the social network of scientific collaborations. Physica A **311**(3–4), 590–614 (2002)
24. Dorogovtsev, S.N., Mendes, J.F.F.: Evolution of networks. Adv. Phys. **51**(4), 1079–1187 (2002)
25. Kuada, E., Olesen, H.: A social network approach to provisioning and management of cloud computing services for enterprises. In: Proc. of Cloud Computing, pp. 98–104 (2011)
26. Balasubramaniyan, V.A., Ahamad, M., Park, H.: CallRank: combating SPIT using call duration, social networks and global reputation. In: Proceedings of Fourth Conference on Email and Anti-Spam (2007)
27. Eagle, N., Pentland, A.S., Lazer, D.: Inferring friendship network structure by using mobile phone data. Proc. Natl. Acad. Sci. USA **106**(36), 15274–15278 (2009)
28. Ankolekar, A., Szabo, G., Luon, Y., Huberman, B.A.: Friendlee: a mobile application for your social life. In: Proceedings of the 11st International Conference on Human-Computer Interaction with Mobile Devices and Services (2009). doi:10.1145/1613858.1613893
29. Huang, J., Nicol, D.: A calculus of trust and its application to PKI and identity management. In: Proceedings of the Symposium on Identity and Trust on the Internet (2009)


**Mucheol Kim** is a Senior Researcher of NTIS Center at Korea Institute of Science and Technology Information since 2011. He received his Bachelor's degree, Master's degree and Ph.D. degree in School of Computer Science and Engineering at Chung-Ang University, in 2005, 2007 and 2012, respectively. His research interests include Information Retrieval, Social Networks, Sensor Networks, Access Control and Semantic Web.

**Sang Oh Park** received the B.S., M.S., and Ph.D. degrees from the School of Computer Science and Engineering at Chung-Ang University, in 2005, 2007, and 2010, respectively. He has been serving as a Senior Researcher of Global Science experimental Data hub Center at Korea Institute of Science and Technology Information since 2012. He served as a Research Professor at the School of Computer Science and Engineering. His research interests include big data system, tape storage system, embedded system, cyber physical system, home network, and Linux system.