2008 International Symposium on Parallel and Distributed Processing with Applications

Trust Management for Ubiquitous Healthcare

Weiwei Yuan, Donghai Guan and Sungyoung Lee*
Kyung Hee University, Korea
{weiwei, donghai, sylee}@oslab.khu.ac.kr

Abstract

As the cornerstone of effective patient-physician relationships in the traditional healthcare infrastructures, trust faces new opportunities and challenges in the ubiquitous healthcare. Ubiquitous healthcare enables the agents acquire more information on trust evaluation through effectively resource sharing. Yet ubiquitous healthcare also lays the agents in a more dynamic and uncertainty environment for the trust evaluations. This paper contributes to develop a distributed trust management for the ubiquitous healthcare. Our trust management infrastructure is responsible for evaluating the trust value and assigning access rights based on the trust value. Based on each agent's confidence of its personal experience on other agents, three naïve Bayes classifier based algorithms are introduced for the trust evaluation: the robust experience algorithm, the weak experience algorithm and the no experience algorithm. The simulation results show the feasibility and effectiveness of our trust management in the ubiquitous healthcare.

1. Introduction

Trust has long been considered as the cornerstone of effective patient-physician relationships in traditional healthcare infrastructure. The need of trust relates to the information asymmetries arising from the specialist nature of medical knowledge as well as the uncertainty and risk regarding the competence and intentions of the medical service providers on whom the patient is dependent [3]. Trust encourages the usage of services and facilitates. It also inspires the reveal of important medical information and has an indirect influence on health outcomes [4].

Ubiquitous healthcare brings trust new opportunities and challenges. On one hand, the agent is able to acquire more information on the trust evaluation in the ubiquitous healthcare. In traditional healthcare collaborations, an agent's trust is based on its own experience and the word-of-mouth experience provided by limited number of acquaintances. The information may be far from enough to reveal the real quality of the target agent, let alone the situations under which no information is available. By connecting computing devices held by all those who had interactions with the healthcare service providers, the ubiquitous healthcare enables more efficient collections and exchanges of the information required by the agent's trust evaluation. On the other hand, the ubiquitous healthcare lays the agent's trust evaluation in a more dynamic and uncertainty environment. Ubiquitous technologies enable large number of agents dynamically be involved in the healthcare system, such as hospitals, GPs, dentists, pharmacies [5]. Compared with the traditional healthcare, an agent has more chances to collaborate with unknown agents. This makes the trust evaluation more difficult.

Up to now, the research on trust is very rare in the ubiquitous healthcare since to involve ubiquitous technologies in the healthcare infrastructure is still in the beginning stage. And to the best of our knowledge, no literature has systemically focused on the trust management in the ubiquitous healthcare.

Our paper contributes to develop a distributed trust management for the ubiquitous healthcare. Our trust management infrastructure is not only capable of evaluating and updating the trust, but also capable of determining the agent's access rights based on the trust. To evaluate the trust in the ubiquitous healthcare, we introduce three naïve Bayes classifier based trust evaluation algorithms according to the agent's experience on the target agent: the robust experience algorithm, the weak experience algorithm and the no experience algorithm.

The rest of the paper is organized as follows. We introduce the trust used in the ubiquitous healthcare in section 2. Our proposed trust management infrastructure is presented in section 3. Simulation

* Corresponding author.

978-0-7695-3471-8/08 $25.00 © 2008 IEEE
DOI 10.1109/ISPA.2008.117

results on our distributed trust management are given in section 4. Section 5 introduces the related work on the trust management. Section 6 concludes the paper.

2. Understanding Trust

Trust is the measure of willingness to believe in an entity based on its competence (e.g. goodness, strength, ability) and behavior within a specific context at a given time. Trust has various properties [9, 10, 17]. Firstly, trust is subjective. It reflects one agent's personal opinion on another. Secondly, trust is asymmetric. Two agents don't need to have same trust in each other. Thirdly, trust is context specific. E.g. a person trusts the ambulance paramedics to access his electronic patient records (EPR) in emergency, but he may not allow them to access his EPR in ordinary cases. Fourthly, trust is dynamic. Trust varies over time due to different reasons, such as the updated experience on the trusted agent, other agents' recommendations and so on.

In this section, we present various aspects of trust: the trust relationship between different agents, the attributes used in the trust evaluation, and how to use trust in the ubiquitous healthcare.

2.1. Using Trust in Ubiquitous Healthcare

We use an emergency response scenario to demonstrate the importance of trust over traditional security mechanisms in ubiquitous healthcare. Trust mechanism ensures more flexible and reliable service usage for different agents, especially the foreign agents.

Alice suffers from a sudden heart attack. She uses her cell phone to call for help. The ubiquitous healthcare system dispatches appropriate ambulance vehicle based on the locale information. When the ambulance is on its way, the ubiquitous healthcare system searches possible first aid providers around Alice based on the registered mobile devices. It is reported that three people are able to give first aid nearby: a lifesaver, an intern and an internist. The lifesaver is able to give Artificial Respiration (AR) and External Chest Compression (ECC). His reputation is r_1. The intern and internist are able to give basic medical treatments as well as AR and ECC. Their reputation is r_2 and r_3 respectively. The information is sent to Alice's cell phone. Alice's cell phone evaluates the trusts on them based on the preset parameters. The trust decision is sent back to the healthcare system and the system contacts with the selected first aid provider and requested him to give a hand. By using trust, Alice is able to flexibly get reliable first aid though short of personal experience on the first aid provider. When heading to Alice, the ambulance paramedic, Bob, is ready to give the emergency treatment. For better treatment, Bob needs to access Alice's electronic patient record (EPR) to make sure if Alice has any contraindication. Bob uses his PDA to send a request to Alice's cell phone along with the credentials including his reputation and the recommendations on him given by other agents. Alice's cell phone evaluates the trust on Bob and assigns appropriate rights to Bob on accessing her EPR. In this case, trust enables Bob flexibly access Alice's EPR though he has never registered to use this data.

2.2. Trust Relationship

Trust is a directional relationship between a *trustor* – the agent that evaluates its trust on the target agent – and a *trustee* – the agent that is the target of the trust evaluation. Trust is often based on the trustor's personal experiences with the trustee. Yet in absence of the personal experiences, the trustor's trust on the trustee always need to base on the recommendations given by different *recommenders* – agents that give recommendations on the trustee based on their interactions with the trustee. For the reliability of the system, in this paper, the trustor only uses the recommendations given by *direct recommenders*– recommenders that had interactions with the trustor. In this paper, we use recommenders to represent direct recommenders for the simplicity. The trustor and the recommender are a kind of "thinking agent [11]", which means that they have the mechanism to evaluate the trusts or give proper recommendations. The trustee can be anything from a person, organization or physical entity, to abstract notions such as information or a cryptographic key [11]. Mutual trust exists when the trustor and the trustee are both "thinking agents".

2.3. Trust Related Attributes

Different attributes influence the trustor's trust evaluation on the trustee. First of all, a trustor is more likely to trust a trustee which had good interactions with it, which introduces the attributes personal experience into the trust evaluation. Moreover, if an agent always has good interactions with other agents, it is indicated that this agent is more trustworthiness. A trustor is more likely to trust this agent even lack of personal experience. This introduces the attribute reputation into our trust evaluation. In addition, when a trustor evaluates its trust on unfamiliar trustees, it refers to the recommendations given by different raters. These attributes are introduced in more details as follows:

1. Personal experience

The personal experience reflects the trustor's prior knowledge on the trustee. It is essential for the trust evaluation. The trustor's personal experiences on other agents are gained by recording the outcomes of pervious interactions between them. The experiences are evaluated by comparing the expected behaviors with the trustees' actual behaviors. The higher personal experience a trustor has on a trustee, the more likely this trustor is willing to trust the trustee.

2. Reputation

Reputation is what is generally said or believed about a person's or thing's character or standing [11]. An agent's reputation reflects a global degree of trustworthiness in an environment. It is a collective measure of trustworthiness based on the recommendations from other agents. The higher reputation an agent has, the more reliable it is. The concept of reputation is closely related to trust, but there are also distinct differences [11]. Trust reflects the trustor's subjective view on the trustee's trustworthiness, whereas reputation is a global score of the trustee's trustworthiness which can be seen by all agents.

A successful reputation mechanism shall meet three requirements: 1) the agents shall be long-lived [12]; 2) reputations shall be updated according to the agents' new trend of trustworthiness; 3) the updated reputations shall affect the trust decision.

3. Aggregated recommendation

In this paper, we use the aggregated recommendation and the reputation as two distinct attributes for the trust evaluations. Though the reputation is also a collective measure of trustworthiness based on the recommendations, it is a global score for all agents. It reflects the community's general opinion on an agent's trustworthiness. The reputation is evaluated and maintained by some service management agent in ubiquitous healthcare. However, each agent has its personal opinions on recommendations, which means that it weights the recommendations different from the service management agent. This introduces the attribute aggregated recommendation into our trust evaluation. The trustee's aggregated recommendation reflects the trustor's personal opinion on trustee's trustworthiness degree. The higher aggregated recommendation the trustee has, the more reliable it is regarded by the trustor.

3. Trust Management

In this section, we propose a trust management infrastructure for the ubiquitous healthcare. The trust management is responsible for: 1) evaluating and updating each agent's trust on other agents, 2) determining the requesting agent's access rights on the basis of trust according to each agent's security policy.

3.1. Trust Evaluation

Trust evaluation can be viewed as the task to predict the value that a target function $f(\mathbf{x})$ takes in a finite set V, where $\mathbf{x}$ is an instance with observed attribute value for attribute $\mathbf{X}$. Here $\mathbf{X} = [X_1, ..., X_n]$ is the attribute used in the trust evaluation, V is trust value set, and f is the algorithm used to evaluate the trust value. Given an instance with observed attribute value x_1 through x_n for $\mathbf{X}$, we use v to represent the value that V takes. To evaluating trust is to get $v = f(\mathbf{x}) = f(x_1, ..., x_n)$.

In this paper, we use the naïve Bayes classifier as the mapping function from the instance of trust related attributes to the trust value.

1. Brief introduction of the naïve Bayes classifier

Naïve Bayes is one of the most effective and efficient classification algorithms. It builds on the assumption of conditional independence of input.

The Bayesian approach classifies the instance by assigning the most probable target value, v_{MAP}, given the attribute values $< x_1 , \ldots , x_n >$ that describe the instance:

$$v_{MAP} = \arg\max_{v \in V}(P(v | x_1, ..., x_n))$$

The naïve Bayes classifier makes the further assumption that the attribute values are conditionally independent. Therefore,

$$v_{NB} = \arg\max_{v \in V}(P(v)\prod_i P(x_i | v))$$

where v_{NB} denotes the target value output by the naïve Bayes classifier; the prior probabilities $P(v)$ and can to be estimated from the training set; the conditional probabilities $P(x_i | v)$ are computed from the training set differently for discrete attribute values and continuous attribute values.

2. The naïve Bayes classifier based trust evaluation

Based on the trustor's confidence of its personal experiences with the trustee, three naïve Bayes classifier based algorithms are used to evaluate the trustor's trust: the *robust experience algorithm*, the *weak experience algorithm* and the *no experience algorithm*. Different attributes are used in these algorithms as shown in Fig. 1. We explain the implementation of each algorithm as fellows.

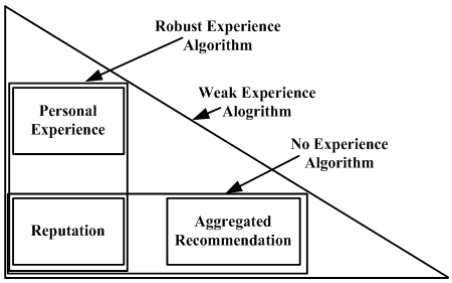


Figure 1: Trust evaluation algorithms.

1) No experience algorithm: the algorithm used for the trust evaluation when the trustor does not have any personal experience on the trustee.

If the trustor is short of personal experience on the trustee, the trust evaluation is based the trustee's reputation and the aggregated recommendation. A trustor *tr*'s trust evaluation algorithm on a trustee *te* in this case is given in the no experience algorithm as follows.

No Experience Algorithm:

Input: $rep(te)$→*te*'s reputation; $rec(te)$→the aggregated recommendation on *te*

Output: $trust(tr, te)$→ *tr*'s trust on *te*;

Variable: $ComNum(tr, te)$→number of communications between *tr* and *te*; *Nb*→naïve Bayes classifier; v →trust value; $P(v)$ →prior probability of v ; $P(.|v)$ → conditional probability of . given v .

if $ComNum(tr, te) = 0$

if there exists recommendations

$$trust(tr, te) = Nb(rep(te), rec(te)) = \arg\max_{v \in V}(P(v)P(rep(te)|v)P(rec(te)|v));$$

end if

end if

2) Robust experience algorithm: the algorithm used for the trust evaluation when the trustor has sufficient personal experience on the trustee.

If the trustor has sufficient personal experience on the trustee, the trust evaluation is mainly based on the trustor's personal experience. A trustor *tr*'s trust evaluation algorithm on a trustee *te* in this case is given in the robust experience algorithm as follows.

Robust Experience Algorithm:

Input: $rep(te)$→*te*'s reputation; $exp(tr, te)$→*tr*'s personal experience on *te*;

Output: $trust(tr, te)$→ *tr*'s trust on *te*;

Variable:

$ComNum(tr, te)$: number of communications between *tr* and *te*; $Thres(tr)$→ *tr*'s threshold value on the number of the communications times; *Nb*→naïve Bayes classifier; v →trust value; $P(v)$ → prior probability of v ; $P(.|v)$ →conditional probability of . given v .

if $ComNum(tr, te) > 0$

if $ComNum(tr, te) >= Thres(tr)$

$$trust(tr, te) = Nb(exp(tr, te), rep(te)) = \arg\max_{v \in V}(P(v)P(exp(tr, te)|v)P(rep(te)|v));$$

end if

end if

3) Weak experience algorithm: the algorithm used for the trust evaluation when the trustor has limited personal experience on the trustee.

If the trustor has limited personal experience on the trustee, in addition to the trustor's personal experience on the trustee, the trustor refers to the recommenders' recommendations on the trustee. A trustor *tr*'s trust evaluation algorithm on a trustee *te* in this case is given in the weak experience algorithm as follows.

Weak Experience Algorithm:

Input: $rep(te)$→ *te*'s reputation; $exp(tr, te)$→ *tr*'s personal experience on *te*; $rec(te)$→ the aggregated recommendation on *te*

Output: $trust(tr, te)$→ *tr*'s trust on *te*;

Variable: $ComNum(tr, te)$→communication times between *tr* and *te*; $Thres(tr)$→ *tr*'s threshold value on the number of the communication times; *Nb*→ naïve Bayes classifier; v →trust value; $P(v)$ →prior probability of v ; $P(.|v)$ →conditional probability of . given v .

if $ComNum(tr, te) > 0$

if $ComNum(tr, te) <= Thres(tr)$

if there exists recommendations

$$trust(tr, te) = Nb(exp(tr, te), rep(te), rec(te)) = \arg\max_{v \in V}(P(v)P(exp(tr, te)|v)P(rep(te)|v)P(rec(te)|v));$$

end if

end if

end if

3.2. Trust Exploitation

Based on the trust value, the trust exploitation is used to determine the requesting agent's access rights according to the trust management policy. A policy is an explicit representation of constraints and rules that govern an agent or system's behavior [15]. The trust management policy used in our paper is shown as follows:

Trust Management Policy:

```
1    verify the trustee's credential;
2    if the credential is valid
3       Acess Right = g(rep(te));
4          if Acess Right >= Request Right
```

```
5              permit;
6            else
7              if ComNum(tr, te) = 0
8                if there is no recommendation
9                  deny;
10               else
11                 call No Experience Algorithm;
12               end
13             else
14               if ComNum(tr, te)>= Thres(tr)
15                 call Robust Experience Algorithm;
16               else
17                 if there is no recommendation
18                   deny;
19                 else
20                   call Weak Experience Algorithm;
21                 end
22               end
23             end
24           end
25     else
26       deny;
27     end
28     Acess Right = g(rep(te)) + h(trust(tr, te),rep(te));
29     if Acess Right >= Request Right
30       permit;
31     else
32       deny;
33     end
```

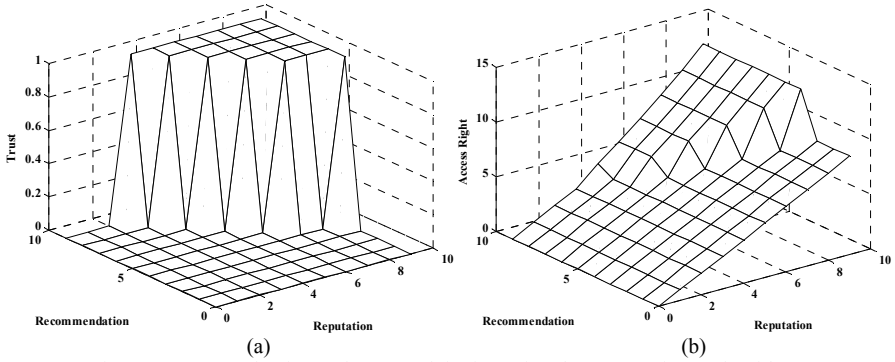
In our trust management policy, access rights are initially related to the reputation of the trustee *te*, i.e., Acess Right = g(*rep*(*te*)), where g(.) is used to represent the mapping from *te*'s reputation to the access rights. If the trustee *te* is trustworthy, additional access rights will be permitted according to its reputation, i.e., Acess Right = g(*rep*(*te*)) + h(*trust*(*tr*, *te*),*rep*(*te*)), where h(.) is used to represent the mapping from *te*'s reputation and trustworthiness to the additional access rights.

4. Simulations

We use the following simulations to show the feasibility and effectiveness of our trust management in the ubiquitous healthcare.

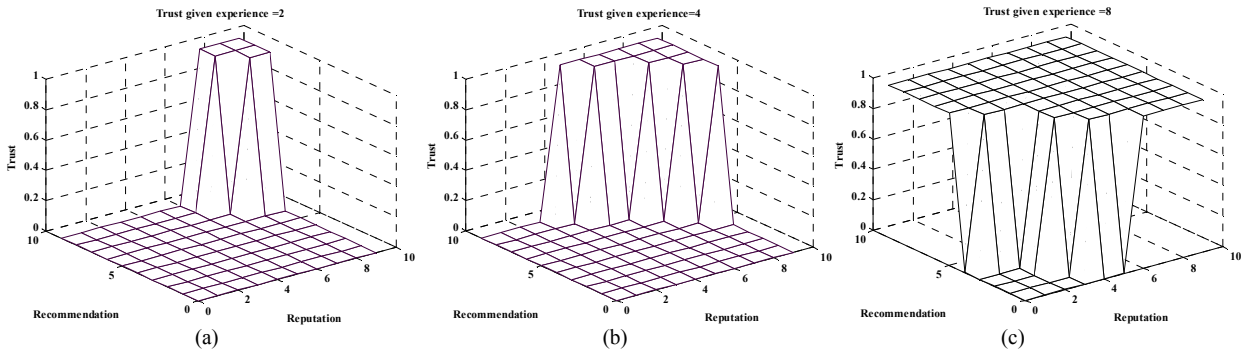
Our simulations are implemented in Matlab. For the no experience algorithm, we randomly generated 1000 instances with the attribute reputation and the attribute aggregated recommendation. For the robust experience algorithm, we randomly generated 1000 instances with the attribute reputation and the attribute personal experience. For the weak experience algorithm, we randomly generated 10000 instances with the attribute reputation, the attribute reputation and the attribute personal experience. In these dataset, the range of the three attributes' value is expressed as integers between 0 and 9. The higher the value is, the higher reputation or aggregated recommendation the trustee has, or the higher personal experience the trustor has on the trustee. We then label these dataset for each algorithm, in which the trust values for labeling are 1 representing trustworthy and 0 representing untrustworthy. The labeled datasets act as the training sets for each naïve Bayes classifier based algorithm.

We further define the access rights mapping function $g(.)$ and the additional access rights mapping function $h(.)$ for trust exploitation module. We use $g(x) = x$ and $h(x, y) = 0.05x^2 y$. The simulation results of the trust evaluation and the trust exploitation using each algorithm are presented in Fig. 2, Fig.3 and Fig.4. Since the naïve Bayes classifiers used by the no experience algorithm and the robust experience algorithm both use two attributes, we only give the simulation results of the no experience algorithm for the simplicity of the paper.



(a) (b)

Figure 2: Trust evaluation and trust exploitation using the no experience algorithm.



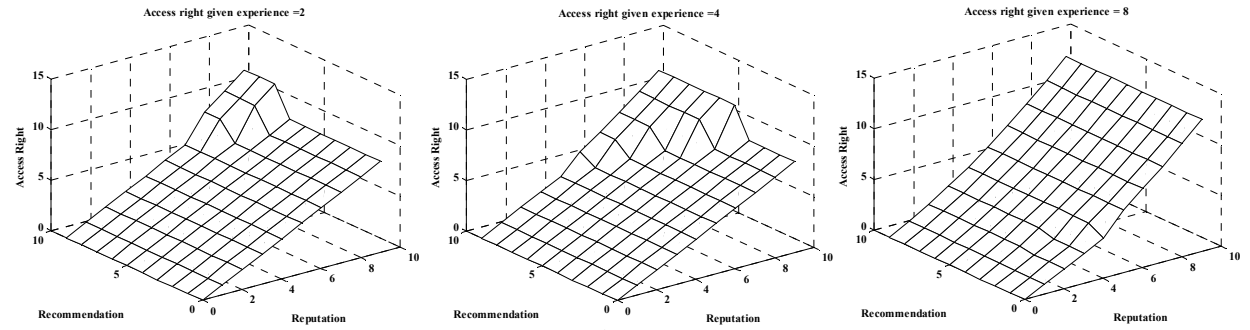
(a) (b) (c)

Figure 3: Trust evaluation using the weak experience algorithm.

Fig. 2a and Fig. 2b show the simulation results of the trust evaluation and the trust exploitation using the no experience algorithm. As shown in Fig. 2a, the trustor's trust on the trustees with the same reputation varies according to the aggregated recommendations on the trustee. And it can be found in Fig. 2b that for the trustees with the same reputation, the trustor may assign different access rights to them. Therefore, compared with assigning access rights merely based on the certificate given by some central authority, as did by the traditional security mechanisms, by using trust management in ubiquitous healthcare, each agent can more flexibly assign access rights to the requesting agent even short of personal experience on the requesting agent. Also, for the agents with the same reputation, since higher aggregated recommendations may contribute to higher access rights, using trust management in ubiquitous healthcare encourages the agents to always behave well when communicating with other agents.

Fig. 3 shows the simulation results of the trust evaluation using the weak experience algorithm. By comparing the sub-figures in Fig. 3, it is clear that the higher personal experience the trustor has on the trusee, the more likely that the trusor trusts the trustee. If the trustor's personal experience on the trustee is very low, even the trustee has good interactions with other agents in the ubiquitous healthcare, e.g. the reputation and the aggregated recommendation equal to 7 in Fig. 3a, the trustor assigns negative trust on the trustee. By contrast, if the trustor's personal experience on the trustee is very high, even the trustee has bad interactions with the other agents, e.g. the reputation and the aggregated recommendation equal to 3 in Fig. 3c, the trustor assigns positive trust on the trustee. This proves that trust is subjective and the personal experience is essential in the trust evaluation.

Fig. 4 shows the simulation results of trust exploitation using the weak experience algorithm, in which each sub-figure is sequentially corresponding to the sub-figures on trust evaluation shown in Fig. 3. It is shown that the higher personal experience the trustor has on the trusee, the more access rights the trustee has compared with the agents with the same reputation and aggregated recommendation. This is because, compared with the agents with the same reputation and aggregated recommendation, the trustee is always regarded as more trustworthy by the trustor if the trustor has higher personal experience on it. Hence in



(a) (b) (c)

Figure 4: Trust exploitation using the weak experience algorithm.

the ubiquitous healthcare, it would lie in the agent's great interests to build up good communications with its frequently requested service providers.

5. Related Work

Though using the trust management in the ubiquitous healthcare is still rare, trust management has been a hot topic in different areas. We give three most widely used trust management applications as follows.

1. Trust in e-business

Trust contributes to the success of e-business [16, 2]. One of the earliest and best known trust systems in e-business is run by eBay, which gathers comments from buyers and sellers about each other after each transaction [1].

The so-called Feedback Forum on eBay is used for domain level trust management. It is a centralized reputation system which evaluates the participant's reputation by collecting all the ratings on the participant and computing the scores. Before participating in the auctions, the new users need to register on the Feedback Forum. User can leave comments about each other after transactions, but are not required to do so. Each comment consists of one line of text, plus a numeric rating of +1 (positive), 0 (neutral), or -1 (negative). The reputation score of each user is the sum of positive ratings minus the sum of negative ratings. And the comments on each user are publicly visible by default, which enables the user to refer to the comments when evaluates its trust. The buyer can then evaluate his trust on the seller based on the seller's reputation, the comments on the seller and his personal experience on the seller (if any).

2. Trust in information retrieval

Trust has been involved in the information retrieval domain to get more reliable and acute information. Google's PageRank [6, 7, 8] is a famous approach based on trust management in this domain.

PageRank selects the best search results based on each page's reputation [8]. This is achieved by using a link analysis algorithm. A single hyperlink to a given web page can be seen as a positive recommendation of that web page. And PageRank ranks a page according to the collection of hyperlinks to a given page. By referring to the hyperlinks given by other pages, PageRank can make more informed decisions. This makes PageRank has the potential to alleviate the general problem of other search engine without the trust mechanism, i.e., the problem of information asymmetry and uncertainty about the page reliability [7]. The rapidly rising popularity of Google has proved the superior search results delivered by the PageRank algorithm using the trust mechanism.

3. Trust in p2p networks

By building the trust of peers, trust management is used to minimize the security threats in p2p networks [9]. Some works have focused on building trust in this domain. And we give two famous examples as follows.

PeerTrust [9] is a reputation-based trust supporting framework. It includes a coherent adaptive trust model for quantifying and comparing the trustworthiness of peers based on a transaction-based feedback system. PeerTrust introduces three basic trust parameters and two adaptive factors in computing trustworthiness of peers, namely, feedback a peer receives from other peers, the total number of transactions a peer performs, the credibility of the feedback sources, transaction context factor, and the community context factor.

EigenTrust [13] is an algorithm used to decrease the number of downloads of inauthentic files in a peer-to-peer file-sharing network. This is achieved by assigning each peer a unique global trust value based on the peer's history of uploads. The algorithm aggregates the trusts by a weighted sum of all raw reputation scores. By having peers use the global trust values to choose the peers from whom they download, EigenTrust effectively identifies malicious peers and isolates them from the network.

6. Conclusions

We have presented a trust management infrastructure for the ubiquitous healthcare which is responsible for evaluating the trust value and assigning access rights based the trust value. Based on the agent's communication history with the requesting agent, the trust management evaluates the trust using three naïve Bayes classifier based algorithms: the robust experience algorithm, the weak experience algorithm and the no experience algorithm. Each algorithm uses different attributes in the trust evaluation including the personal experience, the reputation and the aggregated recommendation. The simulation results proved that the trust management contributes to flexible service access for different agents. Though the research on the trust management in the ubiquitous healthcare is still in the beginning stage, we do believe that the usage of the trust management in the ubiquitous healthcare presents a promising path for the future research.

7. Acknowledgement

This research was supported by the MKE (Ministry of Knowledge Economy), Korea, under the ITRC

(Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Advancement)"(IITA-2008-C1090-0801-0002) and by the MIC (Ministry of Information and Communication), Korea, Under the ITFSIP (IT Foreign Specialist Inviting Program) supervised by the IITA (Institute of Information Technology Advancement, C1012-0801-0003. Also, this work is financially supported by the Ministry of Education and Human Resources Development (MOE), the Ministry of Commerce, Industry and Energy (MOCIE) and the Ministry of Labor (MOLAB) through the fostering project of the Lab of Excellency.

8. References

[1] P. Resnick and R. Zeckhauser, "Trust among strangers in internet transactions: empirical analysis of eBay's reputation system", *the Economics of the Internet and E-Commerce*, vol.11 of Advances in Applied Microeconomics, 2002, Elsevier Science.

[2] V. Shankar, F. Sultan and G. L. Urban, "Online trust and e-business strategy: concepts, implications, and future directions", *Journal of Strategic Information Systems*, vol.11, no.3-4, pp.325-344, Dec. 2002.

[3] R. Rowe and M. Calnan, "Trust relations in health care—the new agenda", *European Journal of Public Health*, vol.16, no.1, pp.4-6(3), Feb. 2006.

[4] D. Safran, D. Taira, W. Rogers et al, "Linking primary care performance to outcomes of care", *Journal of Family Practice*, 47(3), pp.213–220, 1998

[5] N. Dulay, E. Lupu, M. Sloman, J. Bacon, D. Ingram and K. Moody, "CareGrid: autonomous trust domains for healthcare applications", *Magazine of the European Research Consortium for Informatics and Mathematics*, Issue 63, Oct. 2005.

[6] A. Clausen, "The cost of attack of PageRank", *Proc. of The Intl. Conf. on Agents, Web Technologies and Internet Commerce* (IAWTIC'2004), pp.77-90, 2004.

[7] A. N. Langville and C. D. Meyer, "Deeper inside PageRank", *Internet Math*., vol.1, no.3, pp.335-380, 2003.

[8] C. Ridings and M. Shishigin, "PageRank Uncovered", Technical report, 2002.

[9] L. Xiong and L. Liu, "PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities", *IEEE Transactions on Knowledge and Data Engineering* (TKDE), Special Issue on Peer-to-Peer Based Data Management, 2004.

[10] B. Bhargava, L. Lilien, A. Rosenthal, M. Winslett, M. Sloman, T. S. Dillon, E. Chang, F. K. Hussain, W. Nejdl, D. Olmedilla and V. Kashyap, "The pudding of trust", *IEEE Intelligent Systems*, vol.19, no.5, pp.74-88, Sept.-Oct. 2004.

[11] A. Jøsang, R. Ismail and C. Boyd, "A survey of trust and reputation systems for online service provision", *Decision Support Systems*, 43(2), pp.618-644, March 2007.

[12] P. Resnick, R. Zeckhauser, E. Friedman and K. Kuwabara, "Reputation systems", *Communications of the ACM*, 43(12), pp.45–48, 2000.

[13] S. D. Kamvar, M. T. Schlosser and H. Garcia-Molina, "The EigenTrust algorithm for reputation management in p2p networks", *Proc. of the Twelfth International World Wide Web Conference*, 2003.

[14] S. Ruohomaa and L. Kutvonen, "Trust management survey", *Proc. of iTrust 2005*, pp.77-92, 2005.

[15] L. Kagal, T. Finin, A. Joshi and S. Greenspan, "Security and privacy challenges in open and dynamic environments", *IEEE Computer*, vol.39, no.6, pp.89-91, Jun. 2006.

[16] S. Srinivasan, "Role of trust in e-business success", *Journal of Information Management & Computer Security*, vol.12, no.1, pp.66-72, 2004.

[17] L. Kagal, T. Finin, A. Joshi, "Trust-based security in pervasive computing environments", *IEEE Computer*, vol.34, no.12, pp.154-157, Dec. 2001.