A New Dynamic Trust Approach for Cloud Computing

Zhongxue YANG
College of Computer Science and Technology
Nanjing University of Aeronautics and Astronautics
Nanjing, China
School of Mathematic and information Technology
Nanjing Xiaozhuang University
Nanjing, China
young-sir@vip.sina.com

Xiaolin QIN
College of Computer Science and Technology
Nanjing University of Aeronautics and Astronautics
Nanjing, China
qinxcs@nuaa.edu.cn

Yingjie YANG
Centre for Computational Intelligence
De Montfort University
Leicester, UK
yyang@dmu.ac.uk

Wenrui LI
School of Mathematic and information Technology
Nanjing Xiaozhuang University
Nanjing, China
lwr2255@yahoo.com.cn

***Abstract*-Due to highly distributed, non-transparency and dynamic natures of cloud computing, cloud users often confused whether cloud service providers could be trusted. Therefore, a certain trust mechanism or approach should be established to secure a cloud user in selecting a reliable cloud service provider while transactions are taking place. A new dynamic trust approach for cloud computing is proposed in this paper, and multi-level Dirichlet distribution is introduced to compute the value of trust degree. At the same time, confidence factor and time decay factor are taken into account in trust evolution. Simulations are to be set up to observe the performance of the approach, and the results show that the Dirichlet distribution approach for cloud computing is an effective and an efficiency solution in computing the value of trust degree.**

Keywords-Trust; Cloud Computing; Dirichlet Distribution; Confidence Factor; Time Decay factor

I. INTRODUCTION

Cloud computing aims to provide convenient, on-demand, network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services), which can be rapidly provisioned and released with minimal management effort or service provider interactions[1]. As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through the adoption of this new model, which make users anxious about safety and reliability. Users in cloud environment need some mechanisms or approaches to protect data from undesired disclosure. However, traditional approaches or mechanisms based on access control policy are not adequate as they expect that the entities can be statically enumerated and assigned the appropriate privileges in advance. In cloud computing, actually, the entities often do not know each other and need to trust other entities before taking an action. At the same time, the users have to outsource their sensitive data to clouds and feel that they are failure to control over their data, which are generally beyond the same trusted domain as data owners. Moreover, due to highly distributed, non-transparency and dynamic natures of cloud computing, cloud users confuse that whether cloud service providers can be trusted. Thus, it is a significant issue that how to provide trustworthy computing in cloud environment and how to establish a certain mechanism or approach to help cloud users in selecting a reliable service provider.

A new dynamic trust evaluation approach for cloud computing is proposed in this paper and Dirichlet

distribution is introduced to calculate the value of trust degree. The rest of the paper is organized as follows: In section 2, related works of trust are introduced, and trust problem definitions are described in section 3. A dynamic trust approach for cloud computing is proposed and multi-level Dirichlet distribution are introduced to compute the value of trust degree in 4th section, the confidence factor and the time-decay factor are also represented in this section. In the 5th section the simulations and comparatives are made for effectiveness verification of approach. The paper is concluded in the last section.

II. RELATED WORK

Even though trust is a human notion, which is introduced to the area of computer science as the seminal work by Marsh[2], many researches on trust evaluation, however, have been extensively performed for a wide range of applications, such as public key authentication[3],[4], electronics commerce[5], peer-to-peer networks[6], [7], ad hoc and sensor networks [8]–[11]. Trust established in these service environments are successfully used to support users to select the dependable service providers. In recent years, similar issues of establishing trust are already known from cloud computing, and related ideas are needed to support cloud users in selecting trustworthy cloud service providers. Khan KM et al. [12] give an outline of solutions using emerging technologies for establishing trust in cloud computing. Takabi H et al. [13] discuss several security and privacy challenges in cloud computing environments and suggest considering a trust-based framework for supporting adaptive policy integration. Rong Hu et al.[14] propose a trustworthiness fusion model for service cloud platform based on D-S evidence theory and three parties namely service provider, service requestor and service publisher are taken into account to establish a trustworthy service. A trust computing mechanism for cloud computing is proposed by Mohamed Firdhous[15]. The mechanism formulates trust scores for different service level requirements. The mechanism also takes the dynamics of performance variation into computations. Monoj et al.[16] present a trust management architecture which consists of a Cloud Service Registry and Discovery, a Trust Calculator and a Dynamic Trust Monitor which did not take into account the third party providers. Xiaonian Wu[17] describes a trust evaluation model for cloud computing based on the interaction evidence by D-S evidence theory also. However, few of these works focus on providing effective and efficient methods to calculate the value of trust degree and simulations on the well-known security attacks.

The same trust applications based on Dirichlet distribution approach are introduced in the previous researches. K. Thirunarayan et al[18]. provide the method of Dirichlet distribution for direct trust computation and evolution in response to different behaviors in some reputation systems, but not mention cloud computing system. Yang and Cemerlic[19] discuss the approach of Dirichlet distribution to compute reputation to minimize risk in usage control in a collaborative environment. Josang et al[20]. analyze the multi-level reputation system of e-commence by using Dirichlet distribution. Fung et al.[21] use Dirichlet distribution for trust management to collaborative host-based intrusion detection networks to improve security. However, all of works mentioned above do not focus on using the approach of Dirichlet distribution to compute the trust value in cloud computing.

III. PROBLEM DEFINITION

Diego Gambetta[22] defines trust as follows: *'Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action'*. The concept of trust, adjusted to the case of two parties involved in a interaction, can be described as follows: An entity A is considered to trust another entity B when entity A believes that entity B will behave exactly as expected and required. Two entities involved in a interaction can be called *Trustor* and *Trustee*, respectively. In a trusting action, Trustor must decide whether and how much to trust a Trustee based on rather an assessment of its historical experience and the

trustee's reputation than a blind guess.

The *Trust Degree* indicates the trustworthy level of a certain entity which is also classified as two basic trust types, namely, D*irect Trust Degree* and *Indirect Trust Degree*. Direct trust degree is to be updated according to each history-based behavior and experience of the entity in a given context. However, indirect trust degree called *Reputation* also can be associated with many sources of inaccuracy not present in a trustor's direct experience, which is decided by recommendations from other ever given evaluation entities. *Overall trust degree*, in general, is used to evaluate the trustworthy level as well, which is computed according to weighted average value of direct trust degree and indirect trust degree.

In general, trust relationship is variable owing to the *dynamic* nature of interactions and behavior evolution in cloud computing environment. Cloud users trust the ability of cloud service providers to provide services with the increase of their successful interactions. A cloud user will gradually change and adjust its trustworthiness to a cloud service provider as time goes on. Therefore, Trust is a continuous process rather than an isolated action, in which one entity's trust to another is to a certain extent, from low to medium, and then to high, or from high to medium, and then to low.

Trust model in cloud computing has to face many new challenges in contrast with the traditional model due to the diversity of trust relationships in cloud environment, which involves so many different relationships between and among end users, data owners, cloud service providers, and even among other cloud components. That a cloud user trusts a cloud server, in fact, is not equal to that the cloud server does trust the cloud user as well. Here, cloud users might be defined as trustor and Cloud servers or service providers as trustee, and the trustor tries to trust in the ability of trustee to provide some service in accordance with an agreed policy. On the other hand, trustee as a trustworthy party should assure that its resources can be accessed effectively and efficiently by trustor. Without a trustworthy computing environment, service providers will have little incentive to contribute their computing or service resources and cloud users may hesitate to interact with service providers because of the possibility of receiving corrupted or poisoned files or being exploited by malware.

IV. DIRICHLET DISTRIBUTION APPROACH

A. *Dirichlet Distribution for Cloud Computing*

The Dirichlet distribution[23] often denoted $Dir(\alpha)$, is a family of continuous multivariate probability distributions parameterized by α vector a of positive reals. It is the multivariate generalization of beta distribution. Dirichlet distributions are very often used as prior distributions in Bayesian statistics, and in fact the Dirichlet distribution is the conjugate prior of categorical distribution and multinomial distribution. That is, its probability density function (PDF) returns the belief that the probabilities of k rival events are x_i given that each event has been observed $\alpha_i - 1$ times. Let $x = (x_1, ..., x_k)$ be a random probability function, that is $x_i \geq 0$ for $i = 1, 2, ..., k$ and $\sum_{i-1}^{k} x_i = 1$. In addition, suppose that $\alpha = [\alpha_1, ..., \alpha_k]$, with $\alpha_i > 0$ for each i, and let $\alpha_0 = \sum_{i=1}^{k} \alpha_i$. Then, x is said to have Dirichlet distribution with parameter α, which we denote by $x \sim Dir(\alpha)$. The Dirichlet PDF can express as below:

$$f(x_1, \cdots, x_{k-1}; \alpha_1, \cdots, \alpha_k) = \frac{\Gamma(\sum_{i=1}^{k} \alpha_i)}{\prod_{i=1}^{k} \Gamma(\alpha_i)} (\prod_{i=1}^{k} x_i^{\alpha_i - 1})$$

, where $\Gamma(s)$ denotes s the gamma function, which is a generalization of the factorial function and $\Gamma(n) = n\Gamma(n-1) = (n-1)!$ for positive integer n. The mean of a Dirichlet distribution is denoted as $Mean(x_i) = \alpha_i / \alpha_0$ where $\alpha_0 = \sum_{i=1}^{k} \alpha_i$. Dirichlet distribution serves as a conjugate prior for the probability parameter x of the multinomial distribution and permits an efficient way to update the estimated distribution as a result of a new experience by just incrementing the corresponding parameter, which provides a satisfactory mathematical foundation for cloud trust systems that use multilevel trust metric. This important property means the posteriori trust degree can be computed by combining the priori trust

degree with a new interaction experience. While in cloud computing environment, a user is allowed to evaluate a service provider, with any level from a set of predefined k different discrete levels. This translates into having a state space of cardinality k for the Dirichlet distribution. Each trust level can be indexed by i and each x_i is the probability at level i, for a k-level trust space. Note that, for parameters $(\alpha_1,...,\alpha_k)$ where each $\alpha_i - 1$ corresponds to the count of experiences at the level i. The Dirichlet posterior distribution of x after $i-1$ occurrences of level i experience with probability x_i can be represented as $f(x_1,...,x_k;\alpha_1,...,\alpha_{k-1})$ where the prior distribution of x is uniform. Since the Dirichlet distribution is a conjugate prior of the multinomial distribution, the posteriori distribution does also sever the Dirichlet distribution, and stands for addition operation. which usually is also described as shown below:

$$f(x_i \mid \alpha_i, c_i) = \frac{\Gamma(\sum_{i=1}^{k}(\alpha_i + c_i))}{\prod_{i=1}^{k}(\Gamma(\alpha_i + c_i))} \prod_{i=1}^{k}(x_i^{(\alpha_i + c_i - 1)})$$

, where α_i is a base rating value and c_i is a prior constant which is equal to the cardinality of the state space. Then, the distribution of a cloud user's dynamic trustworthiness can be computed using Dirichlet PDF $(\alpha_1, \alpha_2, \cdots, \alpha_k)$ with the count of experience $\alpha_i - 1$ at level i. The best estimate for overall trust degree value is the expectation of probability function, i.e. the mean $(\alpha_1/\alpha_0, \cdots, \alpha_k/\alpha_0)$, and the best estimate for confidence in individual mean is its variance as shown follows: $Variance(x_i) = (\alpha_i \times (\alpha_0 - \alpha_i)) / (\alpha^2 \times (\alpha_0 + 1))$.

The approach based on Dirichlet distribution PDF allows cloud users to update the trust degree value after transactions between cloud users and service providers are taken place. The trust degree level can be characterized by 5-star rating model as signifying *(very untrustworthy, untrustworthy, neutral, trustworthy, very trustworthy)* which is collected from cloud users' feedback. A default base experience value can be assumed to set equal to 1/5 for all levels before any experience score values have been received.

B. *Overall trust degree value*

In our approach, $T_{i,j}(t)$ denotes the overall trust degree value that cloud user i has on cloud service provider j at time t, which is within the range of [0, 1] and with "0" indicating distrust and "1" indicating trust fully. The higher value of $T_{i,j}(t)$ indicates the stronger belief that cloud user i has on service provider j.

Let $D_{i,j}(t)$ and $R_{i,j}(t)$ denote the direct trust degree value and indirect degree (reputation) value that i-user trusts j-provider at time t, respectively. Then, $T_{i,j}(t)$ can be defined as $T_{i,j}(t) = \beta_{i,j} D_{i,j}(t) + (1-\beta_{i,j}) R_{i,j}(t)$, where $\beta_{i,j} \in [0,1]$ is a parameter reflecting the confidence that the user i trusts service provider j directly.

C. *Confidence Factor and Time Factor*

Obviously, the more the number of the interactions among cloud users and service providers, the higher weight the trust degree, and the higher confidence factor which is introduced to estimate the trust degree. It is worth mentioning that the confidence factor level should be maximized if the trust degree is greater than a trust threshold value. For the sake of simplicity and ease of calculation, we define the function as:

$\omega_{i,j} = 1 - \frac{1}{r_{i,j} + c}$, where $r_{i,j}$ is a positive integer or zero which counts the number of transactions between the i-user with the j-provider and c is a constant value which can be preset (usually $c = 2$) by organizer according to the initial value while the first transaction is taking place.

Because of the dynamic characteristic of cloud computing, the indirect trust degree (reputation) between cloud users and service providers will gradually reduce along time increasing. Particularly, if transaction record exceeds a given time interval, reputation trust degree has less weight

than trust degree that calculated finally. Time decay factor $\varphi_{i,j}$ to estimate reputation is defined as $\varphi_{i,j} = \lambda^{\tau_{i,j}}$, where $\tau_{i,j}$ denotes the time stamp of transaction between the i-user and the j-provider and λ is an aging factor $(0 < \lambda \le 1)$. The value of λ is calculated using the decision function[24], as shown below. where $\gamma(\alpha)$ is the comparison function that returns the average ranking distance of all the items. Obviously, the smaller the value of λ, the more emphasis putting on the time decay factor. Meanwhile, the longer the time pasts, the more the trust degree reduces.

Algorithm1: The algorithm for determining the value of the aging factor λ

1: Function Aging_Factor
2: $i \Leftarrow -1$; $\alpha_1 \Leftarrow 1-10^i$; $\delta_1 \Leftarrow \gamma(\alpha_1)$
3: while true do
4: $\alpha_2 \Leftarrow 1-10^{i-1}$; $\delta_2 \Leftarrow \gamma(\alpha_2)$
5: if $|\delta_1 - \delta_2| / \delta_1 \le 0.1$ then
6: Return α_1
7: End if
8: $\alpha_1 \Leftarrow \alpha_2$; $\delta_1 \Leftarrow \delta_2$; $i \Leftarrow i-1$
9: end while

V. SIMULATIONS

In our experiments, the performance and the effectiveness of multi-level Dirichlet distribution approach for cloud computing system are traced and simulated on some well-known attacks.

Bad mouthing attack, ballot-stuffing attack , on-off attack and conflicting behavior attack are used to observed as long as recommendations are taken into consideration.

Table I. Comparative Analysis of Robustness to Attacks

Approach	**Beta-PDF**	**D-S Evidence**	**Our Approach**
Bad Mouthing	Robust	Robust	Robust
Ballot-Stuffing	Weak	Weak	Robust
On-off	Weak	Robust	Robust
Conflicting Behavior	Weak	Weak	Robust

As shown in table above, Dirichlet distribution approach for cloud computing is effective and efficiency on various well-known attacks while comparing with approaches of Beta-PDF and D-S Evidence theory.

VI. CONCLUSION

It is a critical issue to establish a certain trustworthy computing mechanism or approach to help a cloud user in selecting a reliable service provider in cloud environment. The approach of multi-level Dirichlet distribution to compute the value of trust degree for cloud computing is proposed in this paper and the confidence factor and time decay factor are both taking into account for trust evolution. The distribution of a cloud user's dynamic trustworthiness can be computed by using Dirichlet distribution PDF in accordance with the history-based experiences or recommendations. Simulations are to be set up to observe the performance of the approach, and it is shown in the simulations that Dirichlet distribution approach for cloud computing is effective and efficient for a cloud user to compute the value of trust degree.

ACKNOWLEDGEMENT

The authors would like to thank the support by the National Natural Science Foundation of China under Grant (Nos. 61202136) and the Natural Science Foundation of Jiangsu Education Department under grant of the year 2009 and 2012, respectively. The work is supported by Jiangsu Province Scholarships of Overseas Studies under grant of the year 2010.

REFERENCES

[1] Mell P, GranceT, "The NIST definition of cloud computing (draft)," NIST, http://csrc.nist.gov/publications/drafts/800-145/DraftSP-800145_cloud-definition. pdf ; 2011.

[2] S. P. Marsh, "Formalisin Trust as a Computational Concept," Ph.D. Dissertation, University of Stirling, 1994.

[3] A. Jøang, "An algebra for assessing trust in certification chains," Proceedings of the Network and Distributed Systems Security (NDSS'99) Symposium, 1999.

[4] M. Blaze, J. Feigenbaum, J. Lacy, "Decentralized trust management," Proceedings of the 1996 IEEE Symposium on Security and Privacy , pp. 164-173, May 1996.

[5] A. Jsang, R. Ismail, C. Boyd, "A survey of trust and reputation systems for online service provision," Decision Support Systems, 2005.

[6] P. R. Zimmermann, The Official PGP User's Guide, MIT Press, 1995.

[7] S. D. Kamvar, M. T. Schlosser, H. Garcia-Molina, "The eigen trust algorithm for reputation management in p2p networks," Proceedings of 12th International World Wide Web Conferences, May 2003.

[8] S. Buchegger, J. L. Boudec, "Performance analysis of the confidant protocol," Proceedings of ACM Mobihoc , 2002.

[9] P. Michiardi, R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," Communication and Multimedia Security, September 2002.

[10] G. Theodorakopoulos, J. S. Baras, "Trust evaluation in ad-hoc networks," Proceedings of the ACM Workshop on Wireless Security (WiSE'04) , Oct. 2004.

[11] Y. Sun, W. Yu, Z. Han, K. J. Ray Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," IEEE JSAC special issue on security in wireless ad hoc networks, 2006.

[12] Khan KM, Malluhi Q, "Establishing trust in cloud computing," IT Professional 2010(12).

[13] Takabi H, Joshi J, Ahn G, "Security and privacy challenges in cloud computing environments," Security Privacy. IEEE 2010(8),pp24-31.

[14] Rong Hu, Jianxun Liu, Rong Hu, Jianxun Liu, "A Trustworthiness Fusion Model for Service Cloud Platform Based on D-S Evidence Theory," 2011 11th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, 2011, pp566-571.

[15] Mohamed Firdhous, Osman Ghazali, Suhaidi Hassan, "A Trust Computing Mechanism for Cloud Computing," ITU-T Kaleidoscope Academic Conference,2011.

[16] Monoj Kumar Muchahari, Smriti Kumar Sinha, "A New Trust Management Architecture for Cloud Computing Environment," 2012 International Symposium on Cloud and Services Computing, 2012 pp136-140.

[17] Xiaonian Wu, Runlian Zhang, Bing Zeng, Shengyuan Zhou, "A trust evaluation model for cloud computing," Information Technology and Quantitative Management (ITQM2013), 2013, pp1170–1177.

[18] K. Thirunarayan, P. Anantharam, C. Henson, A. Sheth, "Comparative trust management with applications: Bayesian approaches emphasis," Future Generation Computer Systems (2013), http://dx.doi.org/10.10- 16/j.future.2013.05.006.

[19] L. Yang, A. Cemerlic, "Integrating Dirichlet reputation into usage control," Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information. Intelligence Challenges and Strategies (CSIIRW '09), 2009.

[20] Jøsang, J. Haller, "Dirichlet Reputation Systems," The 2nd International Conference on Availability, Reliability and Security (ARES 2007), pp112-119, 2007

[21] J. Fung, J. Zhang, I. Aib, R. Boutaba, "Dirichlet-Based Trust Management for Effective Collaborative Intrusion Detection Networks," Computer Engineering, 8(2), p79-91, 2011.

[22] Gambetta Diego, "Trust: making and breaking cooperative relation," Department of Sociology, University of Oxford, 2000.

[23] B. A. Frigyik, A. Kapila, M. R. Gupta, "Introduction to the Dirichlet Distribution and Related Processes," UWEE Tech Report UWEETR, 2010.

[24] Bo-Chun Wang, Wen-Yuan Zhu, Ling-Jyh Chen, "Improving Amazon-like Review Systems by Considering the Credibility and Time-Decay of Public Reviews," The International Workshop on Web Personalization, Reputation and Recommender Systems, 2008.