Ann Oper Res (2015) 233:281–292
DOI 10.1007/s10479-013-1380-x

A trust model of cloud computing based on Quality of Service

Paul Manuel

Published online: 24 April 2013

Abstract Trust plays an important role in commercial cloud environments. It is one of the biggest challenges of cloud technology. Trust enables users to select the best resources in a heterogeneous cloud infrastructure. We introduce a novel trust model based on past credentials and present capabilities of a cloud resource provider. Trust value is calculated using four parameters such as availability, reliability, turnaround efficiency, and data integrity. A trust management system is proposed implementing this trust model. The paper describes how a service level agreement is prepared combining quality of service requirements of user and capabilities of cloud resource provider. We also demonstrate that our proposed model performs better than the first in first out model and similar trust models.

Keywords Security · Availability · Reliability · Turnaround efficiency · Data integrity · Trust management system · Cloud computing

1 Introduction

Cloud computing is a paradigm that shares computing and storage infrastructure over a scalable network of resources. In the modern world, data are scattered in different data centers and applications are in remote servers. The cloud technology brings the scattered data and the remote applications to user laptop in a virtual form. The main idea is to make computing and storage infrastructure available for cloud users irrespective of time and location. In order to commercialize the cloud technology, cloud users should have the trust that the resource providers complete the submitted job as per the service level agreements (SLA) and the information of the processed data is secured (Abbadi and Alawneh 2012; Krautheim et al. 2010; Zhou et al. 2011). Urquhart (2009) states that the biggest cloud computing issue is trust. Trust plays an important role in all commercial cloud environments and trust management is an integral part of commercial aspects of cloud technology (Noor and Sheng 2011; Messina et al. 2013). Cloud infrastructure supports three types of service delivery models

P. Manuel (✉)
Department of Information Science, Kuwait University, Adeliah, Kuwait
e-mail: p.manuel@ku.edu.kw

such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The cloud service providers offer infrastructure, platform and software to the users in an economical and trustworthy manner.

Trust becomes a complex issue in the cloud-computing arena. Companies like Google and Amazon (Hwang and Li 2010) have implemented reputation based trust management system and it helps the users to locate the trustworthy resource providers for doing e-business transactions in a secure and confident manner. E-bay has a built-in centralized model of trust (Hwang and Li 2010). There are several trust frameworks which are studied in cloud environments (Abbadi and Alawneh 2012; Krautheim et al. 2010; Zhou et al. 2011; Noor and Sheng 2011; Messina et al. 2013).

How is trust measured? When we seek a service from a vendor, we look at two things from the vendor. First, we look at the present capabilities of the vendor whether he can provide good service to us. Second, we look at the past credentials of the vendor. That is, selection process of a vendor consists of two factors: past credentials and present capabilities of the vendor. Past credentials of cloud resource describe the past reputation and service records of the resource. It includes reliability, availability, turnaround time, and data integrity. Present capabilities of cloud resource describe what is offered at present. It includes the present status of *security level* of the environment, *computing power* such as average throughput, processor speed, RAM size, hard disk capacity, *networking strength* such as bandwidth and latency of the resources.

The objective of the paper is to propose a simple and realistic trust model of cloud environments. In this paper, we simplify trust model and derive a formula of trust value of a cloud resource in terms of QoS requirements such as reliability, availability, turnaround time, and data integrity. We also explain how a cloud resource is selected by combining its trust and capabilities. Using simulation, we demonstrate that our proposed model performs better than the first in first out model and similar trust models.

2 How to compute trust value of a resource?

Grandison and Sloman (2000) have surveyed several existing trust models and they have defined the trust as "the firm belief in the capability of an entity to act consistently, securely and reliably within a specified context". They also claim that the trust is the composition of multiple attributes such as reliability, honesty, truthfulness, dependability, security, competence, timeliness, Quality of Service (QoS) and Return on Investment (ROI) in the context of an environment.

As it is mentioned above, we compute trust from the credentials of the resource provider. We consider the credential attributes such as availability, reliability, turnaround efficiency, and data integrity to compute trust value.

Availability (AV):

Availability is the degree to which a system or component is operational and accessible when required for use—IEEE 90 (1990). In software engineering, availability is measured in terms of mean time between failures and mean time to repair (IEEE 90 1990). When a job is submitted to a cloud resource, the resource is said to be *unavailable* in one of the following situations:

1. A part of service of the resource is denied to the user.
2. The resource is shut down.

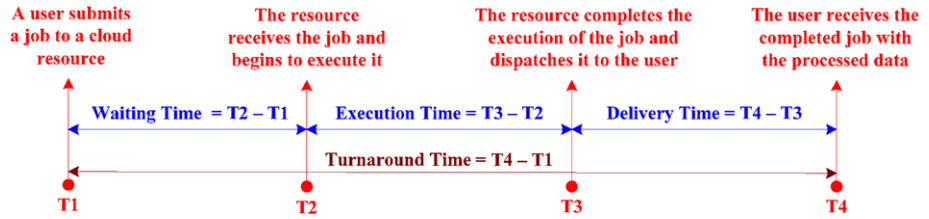

Fig. 1 Turnaround time

3. The resource is too busy to process the job request.

Let us assume that $R_1, R_2, \ldots, R_m$ are the cloud resources. For each $k = 1, 2, \ldots, m$, let N_k denote the number of jobs submitted to cloud resource R_k over a period T. Out of N_k jobs submitted to R_k, let A_k denote the number of jobs accepted by the resource R_k over the period T.

$$\text{Availability of resource } R_k(\text{AV}) = \frac{A_k}{N_k}$$

Reliability (RE):

Reliability is an important component of trust (Gupta et al. 2013). It is also called success rate. Reliability is the ability of a system or component to perform its required functions under stated conditions for a specified period of time—IEEE 90 (1990). Once a cloud resource accepts a job, how reliably does it complete the job? Reliability of a cloud resource is a measure of successful completion of accepted jobs by the cloud resource (Gupta et al. 2013). Out of A_k jobs accepted by resource R_k, let C_k denote the number of jobs completed successfully by resource R_k over the period T.

$$\text{Reliability of resource } R_k(\text{RE}) = \frac{C_k}{A_k}$$

Data Integrity (DI):

A key issue that needs special attention in clouds is security (Chen et al. 2013; Firdhous et al. 2011; Sun et al. 2011; Takabi et al. 2010). Data integrity is a broad term and it includes security, privacy and accuracy of the data. Security includes data safety and accuracy includes data precision (Pearson 2013). Data loss might happen due to poor network latency. Precision loss might happen due to obsolete computing infrastructure. Out of C_k jobs completed successfully by resource R_k, let D_k denote the number of jobs data integrity preserved by resource R_k over the period T.

$$\text{Data Integrity of resource } R_k(\text{DI}) = \frac{D_k}{C_k}$$

Turnaround Efficiency (TE):

The turnaround time is the difference between T4 and T1 (T4–T1) which is explained in Fig. 1. The *actual turnaround time* is the exact time between the submission of a job by a user and the delivery of the completed job to the user. The *promised turnaround time* is the

expected time by a resource provider between the submission of a job and the delivery of the completed job. It is promised by the resource provider to the user in the SLA. This actual turnaround time is normally different from the turnaround time promised by the resource provider in the SLA.

$$\text{Turnaround Efficiency for a job by resource } R_k = \frac{\text{Promised Turnaround time by } R_k \text{ in the SLA}}{\text{Actual Turnaround time by } R_k \text{ to complete the job}}$$

Turnaround efficiency is 1 if the promised turnaround time is greater than the actual turnaround time. Turnaround efficiency of a resource R_k (TE) is the average of turnaround efficiency over all the jobs submitted during the period T. Turnaround efficiency incorporates the Computing Power and Networking Speed (in general, Utilization). In addition, it also incorporates throughput which is the number of transaction per second.

Trust Value of a resource:

$$\text{Trust Value of a resource} = \text{w1} * \text{AV} + \text{w2} * \text{RE} + \text{w3} * \text{DI} + \text{w4} * \text{TE}$$

where w1, w2, w3, and w4 are positive weights of the trust parameters such that $\text{w1} + \text{w2} + \text{w3} + \text{w4} = 1$. The weights of the trust attributes are predetermined based on their priority. For example, $\text{w1} = 0.2$, $\text{w2} = 0.2$, $\text{w3} = 0.5$, $\text{w4} = 0.1$. In this example, data integrity is given the highest priority whereas turnaround efficiency is given the lowest priority.

The basic metric set of trust consists of QoS requirements (Chandrasekar et al. 2012). Since the trust is formulated based on Quality of Service (QoS) requirements, we call this model QoS trust model.

3 Architecture of proposed Trust Management System

Figure 2 describes the proposed trust management system. The *User Interface component* and *Authentication & Authorization Service* involve browsing, registration and perimeter security aspects. The *Catalog Service* is similar to UDDI of web services and it provides the list of cloud resources. The *System Manager* is the heart of the architecture. It coordinates and communicates with other components of the system. The *SLA Manager* is responsible for negotiation and compromises on user's QoS requirements. It is also a node between the System Manager and Trust Manager. It retrieves the trust values of requested cloud resources from the Trust Manager and helps System Manager to shortlist the cloud resources based on trust values. It also prepares and preserves SLA between the user and the cloud resource providers. *Provisioning Service* component is a link between the System Manager and the Middleware Agents. Provisioning tool carves out the IaaS, PaaS and SaaS systems from clouds based on the SLA and provisions a working environment to the cloud user in the form of virtualized system. It may also deploy the required images. The other primary jobs of Provisioning Service component are baseline configuration, subscription, roles, and notification. *Governance Service* takes care of three major jobs: monitoring, metering and billing. Governance sub systems manage and control the resource consumption and allocation. This component also provides a framework for policy enforcement and access control to underlying resources. *Middleware Agent* manages the complete lifecycle of Virtual Machines (VM) including creation, customization, sharing, management, and deployment in an

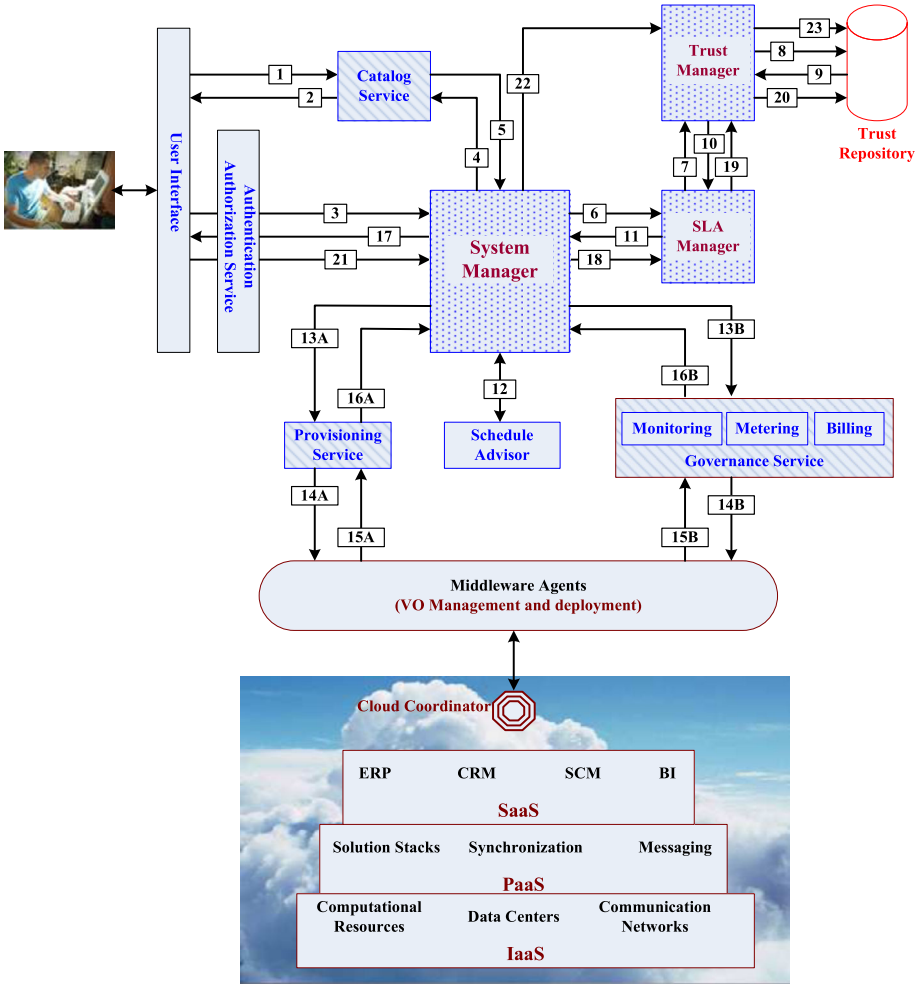

Fig. 2 Architecture of Trust Management System

infrastructure. *Trust Repository* is a database of trust values of cloud resources. *Trust Manager* interacts with the Trust Repository and it stores and processes the trust values retrieved from the trust repository. Each cloud resource has a *Cloud Coordinator* which is an interface between Middleware Agents and the Cloud Resource.

4 Algorithm of Trust Management System:

Steps 1 and 2: A cloud user prepares a list of QoS requirements. The cloud user browses Catalog Service and identifies a set of potential cloud resources.

Step 3: The user submits the list of QoS requirements and a list of potential cloud resources selected from Catalog Service to System Manager.

Steps 4 and 5: The System Manager verifies the availability of the requested cloud resources with Catalog Service.

Step 6: The System Manager forwards the QoS requirements and the list of potential cloud resources to the SLA Manager.

Steps 7, 8, 9, 10, 11: The SLA Manager collects the trust values of the cloud resources from Trust Manager. It sorts the cloud resources based on their trust values. After negotiating and compromising with the cloud user through System Manager, it prepares an SLA. The SLA Manager submits the SLA to System Manager.

Step 12: The System Manager consults Schedule Advisor to schedule the resources.

Steps 13A, 14A, 15A and 16A: The System Manager submits the SLA to the Provisioning Service. The Provisioning Service and the Middleware Agent carve out the requested cloud resource and provision a working environment to the cloud user in the form of virtualized system. They also create, customize, manage and deploy the required virtual systems.

Steps 13B, 14B, 15B and 16B: The System Manager simultaneously submits the SLA to the Governance Service. The Governance Service manages and controls the resource consumption and allocation. It also meters and bills for the cloud service.

Step 17: The System Manager delivers the processed data and the invoice to the user.

Steps 18, 19 and 20: The System Manager also forwards the trust attributes AV, RE, and TE regarding the execution of the job to SLA Manager. The SLA Manager updates the Trust Manager with these values AV, RE, and TE. The Trust Manager in turn stores the data in the Trust Repository.

Steps 21, 22 and 23: After receiving the processed data from the System Manager, the user tests the data and assesses the service rendered by the cloud resource. The user evaluates the data integrity and updates the Trust Manager with the value of DI. The Trust Manager in turn stores the data in the Trust Repository.

5 How to choose a cloud resource given its trust and capabilities?

The QoS has the following factors:

1. *Turnaround time*—time units between the submission of a job and the delivery of the completed job. It is T4–T1. See Fig. 1.
2. *Cost*—the amount in dollar for the subscription of a cloud service.
3. *Security*—it has three levels: Authentication, Authorization and Data Integrity.
4. *Computing Power*—it has three parameters: Processor speed, RAM size, and Hard disk capacity.
5. *Networking Speed*—it has two parameters: Bandwidth and Latency.

Let us assume that cloud user A has the following QoS Requirements:

The user browses catalog service and finds that there are N cloud resource providers $C_1, C_2, \ldots, C_N$ who can provide service meeting his QoS requirements. Then the user submits the list of resource providers $C_1, C_2, \ldots, C_N$ with the list of QoS requirements to System Manager. The System Manager forwards the list of resource providers and QoS requirements to the SLA Manager. The SLA Manager retrieves the trust values of N cloud resources from the Trust Manager and sorts the resources based on the trust values. Here is a sample of two cloud resources C_s, C_t and their capabilities which are given in Table 1 and Table 2.

The capabilities of C_s is better than C_t. On the other hand, the trust value of C_t is better than C_s. It requires trade-off, negotiation and compromise to make a decision. This is done by SLA in consultation with the user A through the System Manager. Let us assume that

Table 1 QoS requirements of cloud user A

QoS factors		QoS required by user A
Turnaround Time		120 minutes
Cost		1000 G$
Security Level	Authentication	LDAP authentication
	Authorization	LDAP authorization
	Data integrity	Data encrypted over network transmission
Computing Power	Processor speed	3.20 GHz Clock Speed 6 MB Cache 533 MHz Bus Speed
	RAM size	2 GB
	Hard disk capacity	640 GB
Networking Speed	Bandwidth	9.6 Gbit/s
	Latency	3.33 milliseconds

Table 2 Capabilities of cloud resource provider C_s and cloud resource provider C_t

Trust value of the resource $C_s = 0.311$

Trust value of resource $C_t = 0.842$

QoS factors		QoS required by user A	Capabilities of resource C_s	Capabilities of resource C_t
Turnaround Time		100 minutes	110 minutes	130 minutes
Cost		1500 $	1500 $	2000 $
Security Level	Authentication	LDAP authentication	Kerberos	Kerberos
	Authorization	LDAP authorization	PERMIS	PERMIS
	Data integrity	Data encrypted over network transmission	Data encrypted using PKI Infrastructure	Data in XML format
Computing Power	Processor speed	3.20 GHz Clock Speed 6 MB Cache 533 MHz Bus Speed	3.60 GHz Clock Speed 8 MB Cache 800 MHz Bus Speed	3.20 GHz Clock Speed 4 MB Cache 600 MHz Bus Speed
	RAM size	2 GB	4 GB	2 GB
	Hard disk capacity	640 GB	8 TB	4 TB
Networking Speed	Bandwidth	9.6 Gbit/s	10 Gbit/s	10 Gbit/s
	Latency	3.33 milliseconds	3.1 milliseconds	4.9 milliseconds

user A decides to select C_t. After negotiation and compromises, an SLA is prepared by SLA Manager. A sample SLA between user A and resource C_t is given in Table 3.

Based on the SLA, cloud resource C_t executes the job and delivers the processed data to user A through the System Manager. After the job is executed, the SLA Manager updates the Trust Manager with the values of AV, RE, and TE (during steps 18, 19). The Trust Manager in turn updates the values in Trust Repository (during step 20). Only the user can test the output data processed by the cloud resource. The user assesses the data integrity and updates the Trust Manager with the value of DI (during steps 21, 22). The Trust manager, in turn, updates Trust Repository with trust value DI of the resource (during step 23).

Table 3 SLA between user A and cloud resource provider C_t

SLA between user A and cloud resource provider C_t		
QoS factors		QoS agreed by user A and resource C_t
Turnaround Time		130 minutes
Cost		2000 $
Security Level	Authentication	Kerberos
	Authorization	PERMIS
	Data integrity	Data in XML format
Computing Power	Processor speed	3.20 GHz Clock Speed 6 MB Cache 533 MHz Bus Speed
	RAM size	2 GB
	Hard disk capacity	640 GB
Networking Speed	Bandwidth	9.6 Gbit/s
	Latency	3.33 milliseconds

6 Experimental setup

"CloudSim provides a generalized and extensible simulation framework that enables modeling, simulation, and experimentation of emerging cloud computing infrastructures and application services, allowing its users to focus on specific system design issues that they want to investigate, without getting concerned about the low level details related to Cloud-based infrastructures and services"—Calheiros et al. (2011). A user submits several jobs where each job is characterized with different capabilities of computational parameters such as different processor speed, hard disk memory, ram memory and network parameters of varying bandwidth and latency to incorporate the heterogeneous concept. The cloud resources are selected by three ways: FIFO model and Combined Trust Model and QoS Model.

FIFO Model: This first-in-first-out model is also called non-trusted model. For each job, a list of cloud resources which meet user QoS requirements is identified. The job is submitted to the first cloud resource in the list.

Combined Trust Model (Manuel et al. 2011): The combined trust is the combination of three popular models such as identity-Based Trust, capability-based trust and behavior-based trust. The combined trust value CT (Manuel et al. 2011) is given below:

$$\mathrm{CT} = a * T_I + b * T_C + c * T_B$$

where $a + b + c = 1$, T_I is identity-Based Trust Value, T_C is capability-based trust value and T_B is behavior-based trust value. For each job, a list of potential cloud resources which meet user QoS requirements is identified. Trust values of these cloud resources are retrieved from the Trust Repository. Then the potential cloud resources are sorted based on their trust values. The job is submitted to the cloud resource of highest trust value from the list.

QoS Trust Model: In order to differentiate our model with other model, we call our model QoS trust model. The QoS trust value QT is given below:

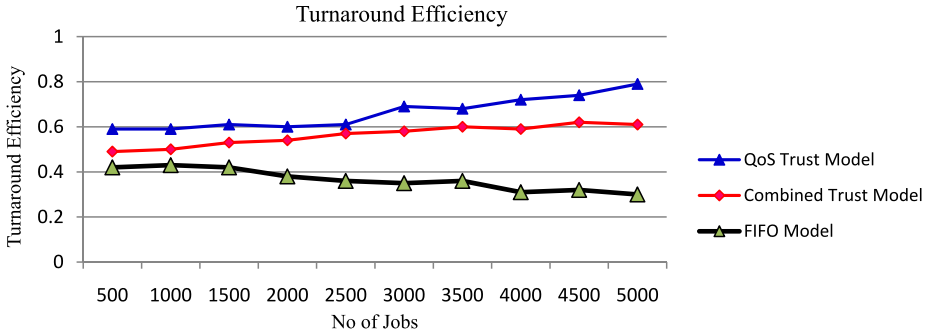

Fig. 3 Turnaround Efficiency

$$QT = w1 * AV + w2 * RE + w3 * DI + w4 * TE$$

where w1, w2, w3, and w4 are positive weights of the trust parameters such that $w1 + w2 + w3 + w4 = 1$. Moreover, AV represents availability, RE represents reliability, DI represents data integrity and TE represents Turnaround Efficiency. As in the previous case, for each job, a cloud resource of highest trust value from the list is selected.

Experiment I—Turnaround Efficiency

Experiment I is a sequence of 10 submissions. Each submission is increased by 500 jobs. During each submission, all the jobs are submitted simultaneously. Here is one example of submission 1 with 500 jobs. The 500 jobs of submission 1 are partitioned into three groups: Group A, Group B and Group C. Each job of Group A uses one database server. Each job of Group B uses two database servers. It retrieves data from both servers, processes the data and writes the output in a flat file. Each job of Group C uses two database servers. It retrieves data from one server and stores the processed data in the second database. Submissions are differentiated by different number of jobs and different database processing. As the number of jobs increase, the experimental results show that QoS model outperforms the other two models. The first experiment demonstrates that our QoS trust model improves turnaround efficiency over FIFO model and combined trust model. See Fig. 3.

Experiment II—Reliability

The second experiment demonstrates that the success rate of our QoS trust model is better than that of other two models. The experiment II is also a sequence of 10 submissions. Submission 1 is a set of 500 jobs. Submission 2 is a set of 1000 jobs. Submission 3 is a set of 1500 jobs and so on. For each submission, the number of jobs is increased by 500 jobs. Submission 10 is a set of 5000 jobs. Here each job requires only one database server. But each job runs different SQL queries. In our experiments, a few jobs fail due to the restriction of the scalability. Some jobs fail when the number of database connection pools is increased. In some cases, jobs fail due to time-out. There are occasions that jobs fail when they write data in flat files. The experimental results in Fig. 4 show that our QoS trust model is better than FIFO model and combined trust model with respect to reliability.

Experiment III—Availability

The third experiment consists of the same sequence of input. In order to measure the availability, we shuffle the number of database servers at random. We also shuffle the servers

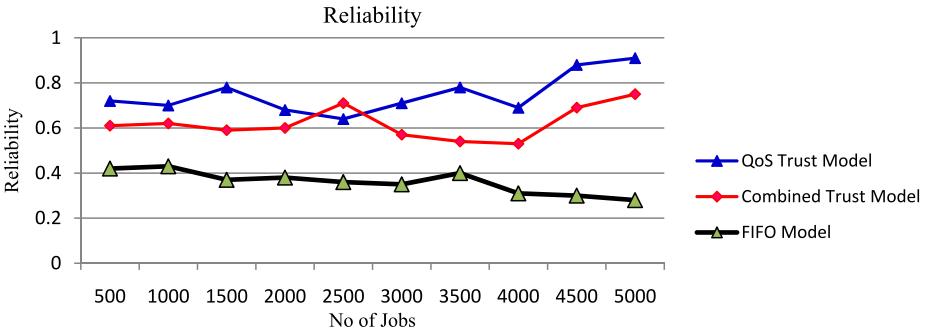

Fig. 4 Reliability

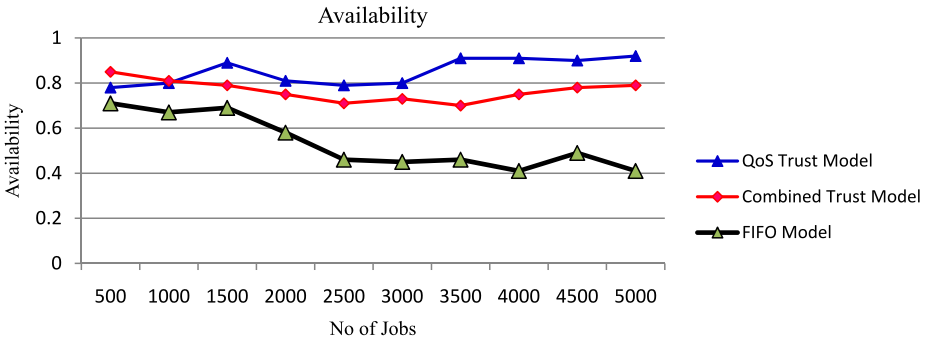

Fig. 5 Availability

among different jobs. Figure 5 shows that QoS trust model is better than the other two models.

Experiment IV—Data Integrity

The fourth experiment consists of the same submissions of jobs. As in the first experiment, the jobs of each submission are partitioned into three groups: Group A, Group B and Group C. The jobs of Group A are measured on privacy. The jobs of Group B are measured on security. The jobs of Group C are measured on accuracy. The output displayed in Fig. 6 reveals that the QoS trust model is better than the other two models with respect to data integrity.

7 Conclusions

We have explained how trust value is calculated based on credential attributes such as availability, reliability, turnaround efficiency and data integrity. We have proposed a novel trust management system called QoS model. We have demonstrated that QoS trust model performs better than the conventional FIFO model and similar trust models. Here trust is measured in terms of four attributes. However, there are some more attributes such as Honesty, Return on Investments and Utilization of Resources. Ko et al. (2011) includes accountability and auditability to measure trust. These parameters are not discussed here. It is interesting

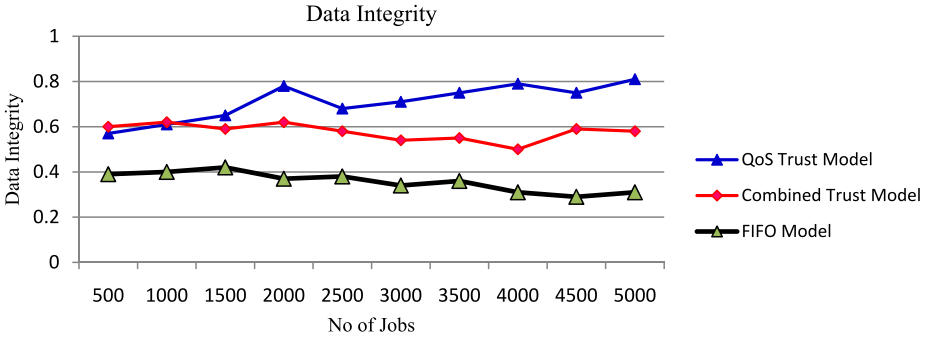

Fig. 6 Data Integrity

to refine trust using these additional attributes. In order to evaluate the performance accurately, we recommend carrying out experiments in a real heterogeneous environment with the combination of MS Platform, UNIX Platform and Linux platform.

Acknowledgement This work is supported by Kuwait University, Research Grant No. [WI 07/11].

References

Abbadi, I. M., & Alawneh, M. (2012). A framework for establishing trust in the cloud. *Computers & Electrical Engineering*, *38*(5), 1073–1087.

Calheiros, R. N., Ranjan, R., Beloglazov, A., De Rose, C. A. F., & Buyya, R. (2011). CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. *Software: Practice and Experience (SPE)*, *41*(1), 23–50.

Chandrasekar, A., Chandrasekar, K., Mahadevan, M., & Varalakshmi, P. (2012). QoS monitoring and dynamic trust establishment in the cloud. In *Lecture notes in computer science: Vol. 7296. Advances in grid and pervasive computing* (pp. 289–301).

Chen, Z., Yao, W., & Wang, C. (2013). Security and trust model for data disaster-recovery service on the cloud, trustworthy computing and services. *Communications in Computer and Information Science*, *320*, 140–147.

Firdhous, M., Ghazali, O., & Hassan, S. (2011). Trust management in cloud computing: a critical review. *International Journal on Advances in ICT for Emerging Regions (ICTer)*, *04*(02), 24–36.

Grandison, T., & Sloman, M. (2000). A survey of trust in Internet applications. *IEEE Communications Survey and Tutorials*. Fourth quarter.

Gupta, P., Kumar Goyal, M., Kumar, P., & Aggarwal, A. (2013). Trust and reliability based scheduling algorithm for cloud IaaS. In *Lecture notes in electrical engineering: Vol. 150. Proceedings of the third international conference on trends in information, telecommunication and computing* (pp. 603–607).

Hwang, K., & Li, D. (2010). Trusted cloud computing with secure resources and data coloring, trust reputation management. *IEEE Internet Computing*, *14*(5), 14–22.

IEEE 90—Institute of Electrical and Electronics Engineers (1990). *IEEE standard computer dictionary: a compilation of IEEE standard computer glossaries*, New York.

Ko, R. K. L., Lee, B. S., & Pearson, S. (2011). Towards achieving accountability, auditability and trust in cloud computing. In *Communications in computer and information science: Vol. 193. Advances in computing and communications* (pp. 432–444).

Krautheim, F. J., Phatak, D. S., & Sherman, A. T. (2010). Introducing the trusted virtual environment module: a new mechanism for rooting trust in cloud computing. In *Lecture notes in computer science: Vol. 6101. Trust and trustworthy computing* (pp. 211–227).

Manuel, P. D., Abd-El Barr, M. I., & Thamarai Selvi, S. (2011). A novel trust management system for cloud computing—IaaS providers. *Journal of Combinatorial Mathematics and Combinatorial Computing*, *79*, 3–22.

Messina, F., Pappalardo, G., Rosaci, D., Santoro, C., & Sarné, G. M. L. (2013). A trust-based approach for a competitive cloud/grid computing scenario. *Studies in Computational Intelligence*, *446*, 129–138. Intelligent distributed computing VI.

Noor, T. H., & Sheng, Q. Z. (2011). Trust as a service: a framework for trust management in cloud environments. In *Lecture notes in computer science: Vol. 6997. Web information system engineering—WISE 2011* (pp. 314–321).

Pearson, S. (2013). Privacy, security and trust in cloud computing, privacy and security for cloud computing. *Computer Communications and Networks*, 3–42.

Sun, D., Chang, G., Sun, L., & Wang, X. (2011). Surveying and analyzing security, privacy and trust issues in cloud computing environments. *Procedia Engineering*, *15*, 2852–2856.

Takabi H., Joshi, J. B. D., & Ahn, G. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, *8*(6), 24–31.

Urquhart, J. (2009). The biggest cloud-computing issue of 2009 is trust. *C-Net News*, 7 Jan. 2009. http://news.cnet.com/8301-19413_3-10133487-240.html.

Zhou, Q., Yu, J., & Yu, F. (2011). A trust-based defensive system model for cloud computing. In *Lecture notes in computer science: Vol. 6985. Network and parallel computing* (pp. 146–159).