Available online at www.sciencedirect.com

ScienceDirect

Karbala International Journal of Modern Science 2 (2016) 203–210
http://www.journals.elsevier.com/karbala-international-journal-of-modern-science/

Trusted services identification in the cloud environment using the topological metrics

Matin Chiregi, Nima Jafari Navimipour*

Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran

Received 7 January 2016; revised 20 June 2016; accepted 21 June 2016
Available online 25 July 2016

Abstract

The trust and reputation in cloud computing are always made only if enough services and expectations are attained. Also, it is a rental for the exploitation of information technology assets and resources. Therefore, this paper evaluates the reputation values and identifies the trusted services in the Cloud environments. The reputation value is evaluated using three parameters including accessibility, dependability, and ability. Also, we propose a method for the trusted service using three topological metrics, including in-degree, out-degree and reputation measures. The proposed method has been evaluated in different challenging situations where the obtained results show that the accuracy of the proposed method using the advice of the trusted service providers is increased.

Index terms: Cloud environment; Trusted service; Reputation; Accessibility; Dependability

1. Introduction

Currently, the Internet puts a huge effect on the society and creates a new revolution in the 21st century where everything and everyone are getting online [1–3]. The cloud computing is a kind of information service made based on a grid and distributed computing [4,5]. It is relatively a new term in information technology [6], firstly popularized in 2006 by Amazon's EC2 [7]. It is a large-scale parallel and distributed computing architecture [8] which promises to bring with itself the great benefits to all types of computing activities [9] and it plays a central role to meet today's business requirements [10]. Also, it is a pervasive computing paradigm that has revolutionized how computer infrastructures and services are delivered [11]. The cloud computing can be seen as one of the latest major evolutions in computing which offers the unlimited possibility to use ICT in various domains [12]. It is the next generation of computer system which extends the network architecture into dynamic and large scale capacity by using the visualization techniques [13]. Major advantages such as the cost reduction and flexibility ensure the cloud computing to be a much-sorted technology in the computing industry [14]. It needs various forms of interactions with entities that are seldom known, and, some parts might never be met [15]. The cloud is a back to the future proposition that was foreseen in the 1950s and is as old as the computing itself [16]. In the cloud environments, the consumers make complex decisions, requiring trust for

* Corresponding author.
E-mail address: jafari@iaut.ac.ir (N.J. Navimipour).
Peer review under responsibility of University of Kerbala.

http://dx.doi.org/10.1016/j.kijoms.2016.06.002

several services and various reasons [17]. The Cloud-based computation services have grown popularity in recent years [18]. It is the Internet-centric providing all the resources and services such as storage, computation, and communication [19]. One of the key promises of the cloud is the speed and ease with which the organizations can temporarily access the additional compute resources [20]. Although the cloud computing services are increasing and gaining popularity, the dread about the usage of the cloud services is still an open issue [21]. The cloud computing offers many advantages by allowing users to apply the infrastructures (for example, servers, networks and storage facilities) and softwares (for example, applications) that are provided by the cloud providers (e.g. Google, Amazon, Expert Cloud, and Salesforce) with pay-per-use fashion and low cost [22,23]. It supports four types of service delivery models, for example, Software as a Service (SaaS) [24,25], Platform as a Service (PaaS) [26], Infrastructure as a Service (IaaS) [27], and Expert as a Service (EaaS) [2,5,28–31].

On the other hand, the trust and reputation between the cloud entities play important roles. It is directly established between the users and service providers [32]. Hence, we can view the trust in the Cloud as the customers' level of confidence in using the Cloud, and try to increase this by mitigating technical and psychological barriers for the Cloud services [33]. The trust is a characteristic considered in all types of the distributed systems for their open and decentralized nature [2]. In other words, the trust is the dependability that two entities have towards each other. For the trusted services and users' gratification in the setting of the cloud computing behavior, the trust of each user should be assessed [34].

The word of "trust" is defined as "a trusted component, operation, or process whose behavior is predictable under almost any operating condition which is highly resistant to the subversion by the application software, viruses, and a given level of physical interference" [35]. It is directly established between the users and Web service providers [32] and can assist the entities to make decisions before establishing collaborations [36].

In this paper, a method to determine the trusted services in the cloud environments is proposed. In the proposed method, the reputation value is evaluated using three parameters including accessibility, dependability, and ability. Also, several methods to identify the trusted service have been proposed using three topological metrics including in-degree, out-degree and reputation.

The rest of the paper is organized as follows: Section 2 discusses the related work. Section 3 introduces the proposed approach. The design and the results of the experiments to test our approaches are described in Section 4. Finally, in Section 5 we point out the conclusions and the future work in this field.

2. Related work

Vişan et al. [37] have proposed an anonymous and secure protocol for keeping, accessing and updating the trust information in decentralized peer-to-peer systems. The system is in a way that the voters have a secret ballot to stay in the system even when the voters have logged out so that the select making process will be fast. The experimental testing has been conducted using Oversim, a flexible simulator.

Also, Adjei et al. [15] have explained the role of the trust in the cloud computing services based on the empirical evidence from interviewing executives of the financial institutions in Ghana. This explanatory paper is based on the literature review and empirical data on exploring reasons for the cloud computing service acquisitions. A combination of interviews focusing on the group discussions was used as methods for the data collection. The information technology and electronic banking executives of the five major commercial banks in Accra, Ghana, between the January and July of 2013 were interviewed. A total of ten respondents were interviewed, two in each of the selected banks. A purposive sampling technique was used in the selection of the informants. This approach allows the selection of qualified informants to ensure extensiveness and diversity of opinion.

Achim et al. [38] have proposed the reputation-based selection of services in the cloud environments. This paper addresses the subject of choosing the right service deployed in a distributed environment for any applications or workflow engines that need access to the best service's endpoint in term of performance. The experimental results highlight the behavior of the offered reputation function and the contrast with the other reputation functions. This paper presents the possibility of enhancing the proposed results in a real environment represented by a workflow engine based on the business process execution language.

Furthermore, Noor et al. [39] have proposed the design and implementation of CloudArmor, the reputation-based trust management framework that provides a set of functionalities to deliver the Trust as a Service (TaaS), which includes: a novel protocol to prove the credibility of trust feedbacks and preserve users' privacy, an adaptive and robust credibility model for measuring the credibility of the trust feedbacks to protect the cloud services from malicious users and to

Table 1
A comparison of the discussed trust mechanisms.

Mechanism	Approach	Result
Vişan et al. [37]	Offering anonymity of the peer that computes and stores the trust value for another peer.	The system is in a way that voters have a secret ballot, votes remain in the system even when the voters have logged out.
Achim et al. [38]	Presenting the possibility for enhancing the proposed solution by a workflow engine.	The behavior of the proposed reputation function and the comparison with other reputation functions.
Adjei et al. [15]	Proposing a mixture of interviews and focusing on the group discussions.	A purposive sampling approach allows the selection of the qualified informants to ensure extensiveness.
Noor et al. [39]	Describing the design and implementation of the CloudArmor.	The feasibility and benefits have been validated by a prototype and experimental studies.
Ding et al. [4]	Proposing a trust model based on the evidence theory.	It proposes a dynamic allocation method of trust weights and gives the calculation method of trust value.
Yan et al. [40]	Proposing a scheme to control data access based on applying the attribute-based encryption.	The results show the efficiency, flexibility for the data access control in the cloud computing.
Ning et al. [41]	Proposing a trusted ring signature scheme based on RSA.	The analysis shows the effectiveness of resolution for the security of the cloud computing nodes.
Tang and Liu [24]	Proposing an FAGI approach.	It offers an objective and efficient way to choose a qualified and trusted cloud service.
Navimipour [2]	Proposing an applicable method for the trustworthy resource discovery.	The proposed method can discover the trustworthy resources efficiently.

compare the trustworthiness of the cloud services, and an availability model to manage the availability of the decentralized implementation of the trust management service. The feasibility and benefits of their approach have been validated by a prototype and experimental studies using a collection of real-world trust feedbacks on the cloud services.

Ding et al. [4] have proposed the trust evaluation research in the Cloud computing involved in the node security communication, security storage, resource allocation and many other aspects. As an effective replacement of the traditional network security, the trust mechanism has effectively solved the security problems of the distributed computing, such as the grid computing, pervasive computing, and ad-hoc networks. The classical trust model and research status of the trust model in the cloud computing have been studied. Considering the factors such as the time, a trust model based on the evidence theory has been proposed in the paper. This model limits the qualification of the entity's recommendation trust proposing a dynamic allocation method of the trust weights giving the calculation method of the trust value.

Also, Yan et al. [40] have proposed a scheme to control data access in the cloud computing based on the trust evaluated by the data owner and/or reputations generated by a number of the reputation centers in a flexible manner by applying the attribute-based encryption and proxy re-encryption. They integrate the concept of context-aware trust and reputation evaluation into a cryptographic system in order to support various control scenarios and strategies. The security and performance of their scheme are evaluated and justified through the extensive analysis, security proof, comparison and implementation. The results show the efficiency, flexibility and effectiveness of their scheme for data to access the control in the cloud computing.

Ning et al. [41] have proposed the anonymous remote attestation based on the property certificate. They obtained the property certificates by matrix replacement algorithm from the platform configuration information and designed a trusted ring signature based on RSA Strong Assumption. By an analysis, the scheme is effective to resolution the security of the cloud computing nodes. Also, they obtained the trusted ring signature scheme based on RSA, which has advantages with the growth of the ring numbers.

Tang and Liu [24] have proposed highlights of the significance and ramifications in a structured selection for a Cloud Service Provider (CSP) in achieving the required assurance level based on an organization's specific security posture. This paper proposes a holistic

model, known as the Function, Auditability, Governability, and Interoperability or FAGI, as an approach to help a Cloud Service Consumer (CSC) to engage and select a trusted CSP through four major decisions. Also, FAGI approach offers an objective and efficient way to choose a qualified and the trusted cloud service and, in turn, saves CSCs' time, effort, and grief.

Finally, Navimipour [2] has proposed a new and applicable method for trustworthy resource discovery in the Expert Cloud by introducing a resource discovery and the trust evaluating method. The proposed method can discover the trustworthy resource efficiently and will be sound, complete, reachable, fair, deadlock-free and consistent.

In this section, the state of the trust mechanism in the cloud computing is studied and some properties of them are defined. In contrast to this paper, we want to provide a precise method to identify the trusted service in the cloud environment using the topological metrics. Table 1 offers the side-by-side comparisons of the reviewed trust mechanisms in the cloud environment.

3. Proposed method

In this section, we first proposed a method to compute the reputation in the cloud environment, then the trusted services in the cloud environment are identified.

3.1. Reputation evaluation

This section proposes a reputation measurement for evaluating the trusted service in a cloud environment. Reputation is an overall estimate of a person or a quality of an entity. In this method, to evaluate the reputation, a mix of several indices has been considered including accessibility, dependability, and ability. To facilitate the description, we firstly define some notations:

- Su denotes the number of jobs submitted over a period T.
- Acc denotes the number of jobs accepted over the period T.
- Com denotes the number of jobs completed successfully over a period T.
- PS denotes the processor speed of resource R.
- MS denotes the memory speed of resource R.
- $Band$ represents the amount of data transferred at the time of the R resource.
- lat represents the delay in reaching R resource.
- PS_{Max} represents the maximum speed of processes existing in the system.
- MS_{Max} represents the maximum speed of memory existing in the system.
- lat_{Min} represents the minimum delay existing in any link of the system.
- We assume that R_1, R_2, …, R_m are the cloud resources.

Accessibility of cloud computing contains the continuous accessibility of the cloud through the cloud profiles, and the ability to synchronize the cloud accessibility preferences. It is as much a submission issue as privacy, safety, and export control. The accessibility of resources R is calculated via Eq. (1).

$$AC_R = \frac{Acc}{Su} \tag{1}$$

Dependability of a cloud is normally defined as "its dependability to deliver a service that can be justifiably trusted" [42]. Dependability in the cloud computing tends to be treated separately because it appears orthogonal; it focuses on the accidental failures. The dependability of resources R is calculated via Eq. (2).

$$DE_R = \frac{Com}{Acc} \tag{2}$$

The current ability of the cloud resources affected the performance of the application execution and file or data transfer [43]. The resource ability describes a quick-growing collection of business and technological capabilities and services obtainable over the cloud. The boundary expresses the state of the art obtainable by the manufacturing members and peers at any given point in time. The ability-based trust value of the resources R is calculated via Eq. (3).

$$AB_R = \frac{((2 \times PS) + MS) + (Band/Lat)}{((2 \times PS_{Max}) + MS_{Max}) + (Band/Lat_{Min})} \tag{3}$$

How to accurately measure the reputation of each cloud service is an imperative research problem in the cloud computing [44]. With the rapid growth of the cloud computing, the importance of a reputation system for the cloud computing services has attracted a lot of attention. Reputation value of an R (REP_R) is evaluated via Eq. (4).

$$REP_R = Weight_1 \times \frac{Acc}{Su} + Weight_2 \times \frac{Com}{Acc} + Weight_3 \times AB_R \tag{4}$$

where $\text{Weight}_1 + \text{Weight}_2 + \text{Weight}_3 = 1$.

3.2. Determining the trusted services

A trusted service plays an important role in the cloud environments. It acts as a safety resource having the ability to influence the public trusted on the subject problem for which the trusted service was known. In this section, we explore the combination of three topological measures, in-degree, out-degree and reputation measure, to identify a group trusted service. The scores for each trusted service as $TS1_R$ and $TS2_R$ is obtained using Eq. (5) or (6).

$$TS1_R = REP_R\left(\left(\alpha \times in\_degree^{+}\right) + (1-\alpha) \times \left(out\_degree^{-}\right)\right) \quad (5)$$

$$TS2_R = REP_R\left(\alpha \times \left(in\_degree^{C} + in\_degree^{IC}\right) + (1-\alpha) \times \left(out\_degree^{C} + out\_degree^{IC}\right)\right) \quad (6)$$

where $\alpha \in (0, 0.1, 0.2, \ldots, 0.9, 1)$, REP_R denotes the reputation, $in\text{-}degree^{+}$ represents the positive opinions that R is taken from other services, $out\text{-}degree^{-}$ represents the negative opinions that R is given to other services, $in\text{-}degree^{C}$ represents the correct opinions that R is taken from other services, $in\text{-}degree^{IC}$ represents the incorrect opinions that R is taken from other services, $out\text{-}degree^{C}$ represents the actual correct opinion that R is given to other services and $out\text{-}degree^{IC}$ represents the incorrect opinion that R is given to other services.

Table 2
Experimental values of the simulations with 300 resources.

Experiment variables	Value
Resources (R)	300
Total number of accepted jobs (*Acc*)	12–18
Total number of submitted jobs (*Su*)	18–25
Total number of successfully completed jobs (*Com*)	6–12
Processor speed (*PS*)	1–100
Memory speed (*MS*)	1–100
The amount of data transferred (*band*)	1–100
The delay to reach R resource (*lat*)	1–100
in-degreec^{-}; in-degreeic^{-}; in-degreec^{+}; in-degreeic^{+}; out-degreec^{-}; out-degreeic^{-}; out-degreec^{+}; out-degreeic^{+}	1–100

4. Experimental results

In this paper, the experiments are developed by using Matlab R2013b and performed on a desktop computer with a configuration such as Intel CPU Core i5, 4 GB RAM, and Windows 7 operating system. In order to test the performance of the proposed method, we use a standard evaluation technique in the cloud environment. In this section, the efficacy of our approach is investigated. We present the details of the extensive experiments on random datasets to evaluate the performance of our approach. The dataset contains 300 resources (R) with different characteristics. The dataset values are described in Table 2. Then, to calculate the reputation, we use three sets of different weights which are shown in three sets in different experiments. Next, according to the obtained results, we select one of the reputations to evaluate the trusted service. Also, we present the results of the selection of the trusted service using the proposed formula. Finally, we compare our methods to other works in the related studies.

We propose several results for the reputation evaluation using different weights. As a first experiment, we consider the reputation weights as $Weight_1 = 0.3$, $Weight_2 = 0.4$, and $Weight_3 = 0.3$. As a second experiment, to investigate the other situations, we change the weights of reputation to $Weight_1 = 0.3$, $Weight_2 = 0.3$, and $Weight_3 = 0.4$. As a third experiment, we consider the weights of reputation as $Weight_1 = 0.4$, $Weight_2 = 0.3$, and $Weight_3 = 0.3$. The obtained results for reputation evaluation in these cases are illustrated in Table 3 and Fig. 1.

We measure the impact of the different trusted service methods and compare the behavior of the implemented methods. There are two methods to

Table 3
Reputation evaluation for each resource.

R	First experiment $Weight_1 = 0.3$, $Weight_2 = 0.4$, $Weight_3 = 0.3$	Second experiment $Weight_1 = 0.3$, $Weight_2 = 0.3$, $Weight_3 = 0.4$	Third experiment $Weight_1 = 0.4$, $Weight_2 = 0.3$, $Weight_3 = 0.3$
1	0.5705	0.5296	0.5572
2	0.5129	0.4895	0.5407
3	0.5179	0.4861	0.5459
⋮	⋮	⋮	⋮
300	0.5556	0.5207	0.5542

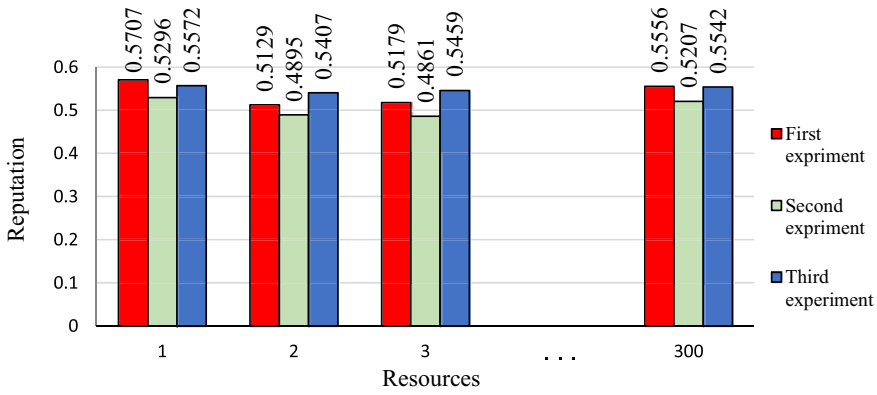

Fig. 1. The reputation values for resources.

recognize the trusted service. We evaluate each of them with two different reputation thresholds. The experiment was conducted for 300 services in the Cloud environment. We analyze the different weights and alpha values. With a hybrid measurement with different alphas, the values are changed only marginally. We consider the subjective alpha values as $\alpha = 0.2$ for each criterion. We consider reputation weights as $\text{Weight}_1 = 0.3$, $\text{Weight}_2 = 0.4$ and $\text{Weight}_3 = 0.3$. We consider this case as a more efficient solution than others. Also, we evaluate this approach using three different reputation thresholds (RE), including 0.6, 0.65, 0.7 and consider the *TS*1 and *TS*2 of $\lambda_{TS} > 50$. The obtained results for the trusted service selection using the two methods are shown in Table 4 and Fig. 2. Also, Fig. 3 demonstrates the percentage of the trusted service identified using the different thresholds.

The results show that if we increase the reputation threshold, the number of the trusted services is decreased. Also, if we increased the value of λ_{TS}, the detected trusted services are decreased. For example, the 95% of the trusted services are detected with RE > 0.6 in TS2 identified 10% more than TS1 with RE > 0.6 or 65% of the trusted service with RE > 0.65 in TS2 that it identified 5% more than TS1. Therefore, TS2 with RE > 0.6 obtains a high percentage of detecting trusted service. Also, the comparative review between the proposed method and the related work is shown in Table 5.

Table 4
Trusted service identification with different weights.

Weight	Name	RE > 0.6 $\lambda_{TS>50}$	RE > 0.65 $\lambda_{TS>50}$	RE > 0.7 $\lambda_{TS>50}$
$\text{Weight}_1 = 0.3$,	TS1	100	58	26
$\text{Weight}_2 = 0.4$, $\text{Weight}_3 = 0.3$	TS2	125	67	28

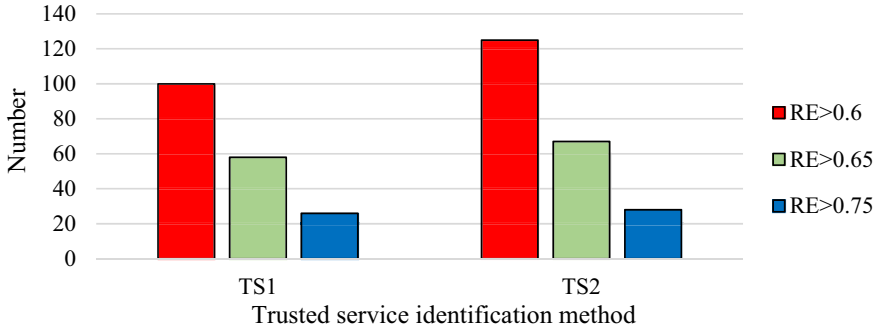

Fig. 2. Trusted service identification using different methods.

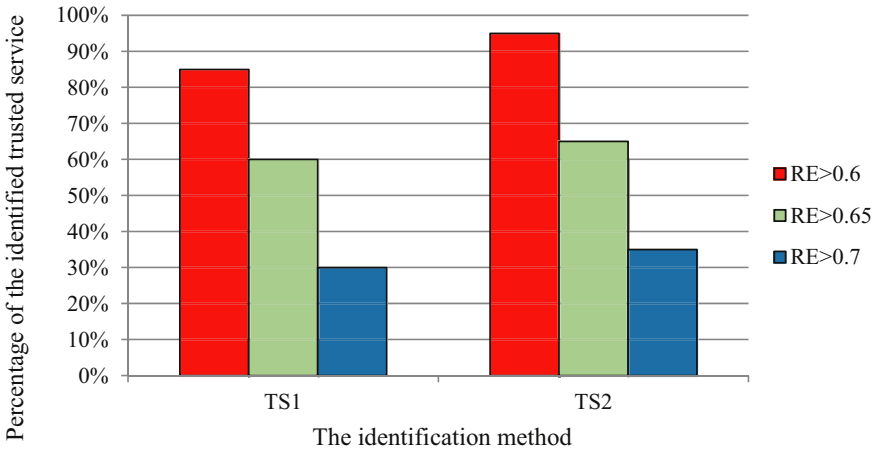

Fig. 3. Percentage of identified trusted service using different methods.

Table 5
Comparative study of proposed method with methods of the related work.

Mechanisms	Trust	Reputation	Accessibility	Dependability	Ability
Proposed method	✓	✓	✓	✓	✓
Vişan et al. [37]	✓	✓	✓	✓	✗
Achim et al. [38]	✓	✓	✓	✗	✗
Adjei et al. [15]	✓	✗	✓	✗	✓
Noor et al. [39]	✓	✓	✓	✗	✓
Ding et al. [4]	✓	✗	✗	✓	✗
Yan et al. [40]	✓	✓	✓	✗	✗
Ning et al. [41]	✓	✗	✗	✗	✗
Tang and Liu [24]	✓	✗	✓	✗	✓
Navimipour [2]	✓	✓	✓	✓	✗

As shown in Table 5, in most of the related work, just some options in the field of the trusted service identification are studied. For example, Ning et al. [41] have considered just the trust, and Ding et al. [4] have considered the trust and dependability. Also, the results show that the provided method acts well than the other related work.

5. Conclusion and future work

In this paper, we propose a new method for the trusted service identification in the cloud environment. We have explained how the reputation value is calculated based on the credential attributes such as accessibility, dependability, and ability. Also, we calculate the trust value using three topological measures including in-degree, out-degree and reputation, while the weights of the trusted services are varied in the Cloud environment. Furthermore, we conclude that the number of the trusted services have a direct relationship to the reputation. If we increase the threshold of reputation value, the fewer number of the trusted service will be selected. Also, we show that the accuracy of the proposed method using the advice of the trusted service is increased. In the future, we plan to investigate the impact of other algorithms on the trust as well as the reputation evaluation. Also, the formal verification and specification of the proposed trust evaluation mechanism in the Cloud environment is still very challenging.

References

[1] B. Nguyen, L. Simkin, The dark side of CRM: advantaged and disadvantaged customers, J. Consum. Mark. 30 (2013) 17–30.
[2] N.J. Navimipour, A formal approach for the specification and verification of a trustworthy human resource discovery mechanism in the Expert Cloud, Expert Syst. Appl. 42 (2015) 6112–6131.
[3] N.J. Navimipour, Z. Soltani, The impact of cost, technology acceptance and employees' satisfaction on the effectiveness of the electronic customer relationship management systems, Comput. Hum. Behav. 55 (2016) 1052–1066.
[4] H. Ding, X. Li, C. Gong, Trust model research in cloud computing environment, in: 2015 International Symposium on Computers & Informatics, 2015.
[5] A.H. Navin, N.J. Navimipour, A.M. Rahmani, M. Hosseinzadeh, Expert grid: new type of grid to manage the human resources and study the effectiveness of its task scheduler, Arabian J. Sci. Eng. 39 (2014) 6175–6188.

[6] K. Mogouie, M.G. Arani, M. Shamsi, A novel approach for optimization auto-scaling in cloud computing environment, Int. J. Mod. Educ. Comput. Sci. 7 (2015).
[7] I.M. Abbadi, A. Martin, Trust in the cloud, Inf. Secur. Tech. Rep. 16 (2011) 108–114.
[8] C. Chawla, I. Chana, Day-Ahead Pricing Model for Smart Cloud Using Time Dependent Pricing, 2015.
[9] V. Chang, R.J. Walters, G.B. Wills, Organisational sustainability modelling—an emerging service and analytics model for evaluating cloud computing adoption with two case studies, Int. J. Inf. Manag. 36 (2016) 167–179.
[10] A. Shameli-Sendi, M. Pourzandi, M. Fekih-Ahmed, M. Cheriet, Taxonomy of distributed denial of service mitigation approaches for cloud computing, J. Netw. Comput. Appl. 58 (2015) 165–179.
[11] H.M. Sabi, F.-M.E. Uzoka, K. Langmia, F.N. Njeh, Conceptualizing a model for adoption of cloud computing in education, Int. J. Inf. Manag. 36 (2016) 183–191.
[12] F. Pop, M. Potop-Butucaru, ARMCO: advanced topics in resource management for ubiquitous cloud computing: an adaptive approach, Future Gener. Comput. Syst. 54 (2016) 79–81.
[13] M. Saad, M. Izuan, K. Abd Jalil, M. Manaf, Achieving trust in cloud computing using secure data provenance, in: Open Systems (ICOS), 2014 IEEE Conference on, 2014, pp. 84–88.
[14] M. Thamizhselvan, R. Raghuraman, S.G. Manoj, P.V. Paul, A novel security model for cloud using trusted third party encryption, in: Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on, 2015, pp. 1–5.
[15] J.K. Adjei, C. Blackman, C. Blackman, Explaining the role of trust in cloud computing services, info 17 (2015).
[16] P. Ryan, S. Falvey, Trust in the clouds, Comput. Law Secur. Rev. 28 (2012) 513–521.
[17] F.Z. Filali, B. Yagoubi, Global trust: a trust model for cloud service selection, Computing 3 (2015) 19.
[18] Y. Wang, J. Wei, Toward protecting control flow confidentiality in cloud-based computation, Comput. Secur. 52 (2015) 106–127.
[19] Y.A. Younis, K. Kifayat, M. Merabti, An access control model for cloud computing, J. Inf. Secur. Appl. 19 (2014) 45–60.
[20] C. Everett, Cloud computing – a question of trust, Comput. Fraud Secur. 2009 (2009) 5–7.
[21] R. Shaikh, M. Sasikumar, Trust model for measuring security strength of cloud computing service, Procedia Comput. Sci. 45 (2015) 380–389.
[22] N. Moghadasi, M.G. Arani, M. Shamsi, A novel approach for reduce energy consumption in mobile cloud computing, Int. J. Comput. Netw. Inf. Secur. IJCNIS 7 (2015) 58.
[23] M.I. Alam, M. Pandey, S.S. Rautaray, A comprehensive survey on cloud computing, Int. J. Inf. Technol. Comput. Sci. IJITCS 7 (2015) 68.
[24] C. Tang, J. Liu, Selecting a trusted cloud service provider for your SaaS program, Comput. Secur. 50 (2015) 60–73.
[25] Y.-D. Lin, M.-T. Thai, C.-C. Wang, Y.-C. Lai, Two-tier project and job scheduling for SaaS cloud service providers, J. Netw. Comput. Appl. 52 (2015) 26–36.
[26] J. Anselmi, D. Ardagna, M. Passacantando, Generalized Nash equilibria for SaaS/PaaS clouds, Eur. J. Oper. Res. 236 (2014) 326–339.
[27] P. Manuel, A trust model of cloud computing based on quality of service, Ann. Oper. Res. (2013) 1–12.
[28] N.J. Navimipour, A.H. Navin, A.M. Rahmani, M. Hosseinzadeh, Behavioral modeling and automated verification of a cloud-based framework to share the knowledge and skills of human resources, Comput. Ind. 68 (2015) 65–77.
[29] N.J. Navimipour, A.M. Rahmani, A.H. Navin, M. Hosseinzadeh, Expert Cloud: a cloud-based framework to share the knowledge and skills of human resources, Comput. Hum. Behav. 46 (2015) 57–74.
[30] N. Jafari Navimipour, A. Masoud Rahmani, A. Habibizad Navin, M. Hosseinzadeh, Job scheduling in the Expert Cloud based on genetic algorithms, Kybernetes 43 (2014) 1262–1275.
[31] M. Ashouraie, N. Jafari Navimipour, M. Ramage, P. Wong, Priority-based task scheduling on heterogeneous resources in the Expert Cloud, Kybernetes 44 (2015).
[32] S.H. Sharif, S. Mahmazi, N.J. Navimipour, B.F. Aghdam, A review on search and discovery mechanisms in social networks, Int. J. Inf. Eng. Electron. Bus. 5 (2013).
[33] R.K. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, et al., TrustCloud: a framework for accountability and trust in cloud computing, in: Services (SERVICES), 2011 IEEE World Congress on, 2011, pp. 584–588.
[34] S.B. Hosseini, A. Shojaee, N. Agheli, A new method for evaluating cloud computing user behavior trust, in: Information and Knowledge Technology (IKT), 2015 7th Conference on, 2015, pp. 1–6.
[35] Z. Shen, L. Li, F. Yan, X. Wu, Cloud computing system based on trusted computing platform, in: Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on, 2010, pp. 942–945.
[36] S. Mohammad Aghdam, N. Jafari Navimipour, Opinion leaders selection in the social networks based on trust relationships propagation, Karbala Int. J. Mod. Sci. 2 (2016) 88–97.
[37] A. Vişan, F. Pop, V. Cristea, Decentralized trust management in peer-to-peer systems, in: Parallel and Distributed Computing (ISPDC), 2011 10th International Symposium on, 2011, pp. 232–239.
[38] O.-M. Achim, F. Pop, V. Cristea, Reputation based selection for services in cloud environments, in: Network-based Information Systems (NBiS), 2011 14th International Conference on, 2011, pp. 268–273.
[39] T. Noor, Q. Sheng, L. Yao, S. Dustdar, A. Ngu, CloudArmor: supporting reputation-based trust management for cloud services.
[40] Z. Yan, X. Li, M. Wang, A. Vasilakos, Flexible data access control based on trust and reputation in cloud computing.
[41] Z.-H. Ning, W. Jiang, J. Zhan, P. Liang, Property-based anonymous attestation in trusted cloud computing, J. Electr. Comput. Eng. 2014 (2014).
[42] A. Chilwan, Dependability Differentiation in Cloud Services, 2011.
[43] M. Chiregi, N.J. Navimipour, A new method for trust and reputation evaluation in the cloud environments using the recommendations of opinion leaders' entities and removing the effect of troll entities, Comput. Hum. Behav. 60 (2016) 280–292.
[44] S. Wang, J. Wei, L. Sun, Q. Sun, F. Yang, Reputation measurement of cloud services based on unstable feedback ratings, in: Parallel and Distributed Systems (ICPADS), 2013 International Conference on, 2013, pp. 474–479.