Computer and Information Science; Vol. 12, No. 3; 2019
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

A Proposition of Modifications and Extensions of Cloud Computing Standards for Trust Characteristics Measures

Sara Moazzezi Eftekhar[1] & Witold Suryn[1]

[1] École de technologie supérieure, Montréal, Canada

Correspondence: Witold Suryn, Department of Software and IT Engineering, École de Technologie Supérieure – ÉTS, Montréal, QC., H3C 1K3, Canada.

Received: April 13, 2019 Accepted: May 7, 2019 Online Published: July 25, 2019

doi:10.5539/cis.v12n3p27 URL: https://doi.org/10.5539/cis.v12n3p27

Abstract

In recent years, we have witnessed a marked rise in the number of cloud service providers with each offering a plethora of cloud services with different objectives. Gaining confidence for cloud technology adoption as well as selecting a suitable cloud service provider, both require a proper evaluation of cloud service trust characteristics. Hence, the evaluation of cloud services before used by the customer is of utmost importance. In this article, we adapt the extracted trust characteristics from both system and software quality standards and cloud computing standards, for evaluating cloud services. Moreover, we derive measures for each trust characteristics to evaluate the trustworthiness of different cloud service providers, and generalize these trust measures for any type of cloud services (e.g. Software as a Service, Platform as a Service, and Infrastructure as a Service). Our work thereby demonstrates a way to apply generalized trust measures for cloud services and therefore contributes to a better understanding of cloud services to evaluate their quality characteristics. As part of our ongoing research, the results of this study will be used to develop a comprehensive cloud trust model.

Keywords: evaluating trust, quality characteristics, measurement, trustworthiness

1. Introduction

In the new global information technology, trust has become a central issue for many organizations and individuals. Evidence suggests that trust is among the most important factors for establishing a relationship and adoption of technology such as cloud computing. Although, more than two decades have elapsed from the first day of introducing cloud computing, unlike the various evolutions and progressions in this technology, trust and trustworthiness are still major concerns and open issues. There is a growing body of literature that recognizes the importance of trust and evaluating the trustworthiness of the cloud service providers (e.g. (Chahal & Singh, 2017; Li, Liao, Leung, Li & Li, 2017; Rajendran & Swamynathan, 2016)). The main challenge faced by many researchers is that the notion of trust is combined with uncertain concepts and at the same time associated with functional and non-functional requirements. This causes that trust in cloud computing remains an obstacle for cloud technology adoption.

On the other hand, there is no consensus based rule or agreed standard to evaluate trust in cloud environments (Eftekhar, Suryn, Roy & Terfas, 2018). In cloud computing standards the key characteristics of cloud have been defined and several concepts related to this technology have been explained (ISO/IEC, 2014). However, there is no clear path to guide stakeholders or individuals toward a trustworthy cloud service provider. An essential question that needs to be asked is “what are the influential characteristics that cover different aspects of trust and users’ requirements?” To answer this question, many researchers proposed several trust characteristics, but they are not sufficient enough to boost users’ confidence in applying cloud technology. For example, in the majority of scientific publications, security is first and foremost trust characteristic that needs to be tackled from different perspectives (e.g. (Gonzales, Kaplan, Saltzman, Winkelman & Woods, 2017)). Undoubtedly, security is a major challenge in cloud computing, but it is important to bear in mind that it is one of the various aspects of trust.

Moreover, a significant part of a reasonable evaluation of trust in cloud environments pertains to evaluating the measures of quality characteristics that are proposed as trust characteristics. Most studies in the field of evaluating trust in cloud computing have only focused on the limited number of trust characteristics with inappropriate selection of measures. However, the selected measures do not necessarily conform to the standards. Hence, extensive research has shown that there is an urgent need to address these trust characteristics along with their measures which can be supported scientifically. In (Eftekhar et al., 2018) the basic set of trust characteristics based on the system and software quality standards and cloud computing standards were derived. Therefore, their measures need to be aligned with them according to the related standards. In this paper, the trust characteristics presented in the work (Eftekhar et al., 2018) are completed and presented with their measures. One of our main goals is to ensure that trust measures conform to standards. Because having an accurate evaluation of trust in cloud environments depends on two principles:1-regorous selection of the trust characteristics and 2- specifying their measures to address all the users' requirements and consider different aspects of trust.

The remaining part of the paper proceeds as follows: Section 2 defines the concepts of trust and trustworthiness and presents a brief explanation of the relationship between these two concepts. Section 3 explains the related research. Section 4 describes the main characteristics with their measures to evaluate trust in cloud environments. Section 4 is discussing results and discussion. Section 5 concludes the paper.

2. Trust and Trustworthiness

It has commonly been assumed that trust is a sophisticated phenomenon (Huang & Nicol, 2013). Not only are there various definitions of trust in literature, but also people have different attitudes toward it (Singh & Sidhu, 2017). Basically, in cloud computing, defining the notion of trust depends on realizing functional and non-functional quality requirements. This shows a need to be explicit about exactly what is meant by the word 'trust'.

Broadly speaking, trust can be defined as a bilateral relationship between a cloud user and a cloud provider. Previous studies mostly defined 'trust' as a psychological state that consists of (Fan, Yang, Perros, & Pei, 2015; Huang & Nicol, 2013; Singh & Sidhu, 2017; Sztompka, 1999):

1- Expectancy- that is related to a particular behaviour from the trustee which is expected by a trustor (e.g. performing the required tasks effectively).
2- Belief- the trustor is in the belief that based on the evidence such as competence and goodwill of the trustee, expected behaviour will be occurred.
3- Have a tendency to take risk- Based on that belief, the trustor has a tendency to take risk.

It is a widely held view that trust is an uncontrollable and intangible concept (Özer & Zheng, 2017). There is a great volume of published studies describing the roles of many influential characteristics contributing to establishing a trust relationship (Habib, Hauke, Ries & Mühlhäuser, 2012). What we know about trust in cloud computing is largely based upon empirical studies that investigate how these characteristics impact the relationship between two entities in cloud environments.

On the other hand, it is now well established from a variety of studies that trust is a measure of trustworthiness (Suryn, 2013). As Suryn (Suryn, 2013) argues, "Trustworthiness is an attribute of an entity deserving of trust or confidence, being dependable and reliable." Regarding this definition, although Suryn in this work identifies credibility, reliability and dependability as the three significant characteristics for trustworthiness, convincing the users, particularly the corporate industrial customers, to broadly adopt cloud technology requires a larger list of characteristics (Eftekhar et al., 2018; Suryn, 2013).

As mentioned earlier, trustworthiness can be measured by trust. Therefore, a possible explanation for the existing relationship between trustworthiness and trust in cloud environments can be depicted as in Figure 1. It is almost certain that the more evaluated characteristics, the greater trustworthiness for the cloud service provider can be achieved. In other words, by measuring these characteristics that are the users' requirements representatives, a trustworthy cloud service provider can be identified.

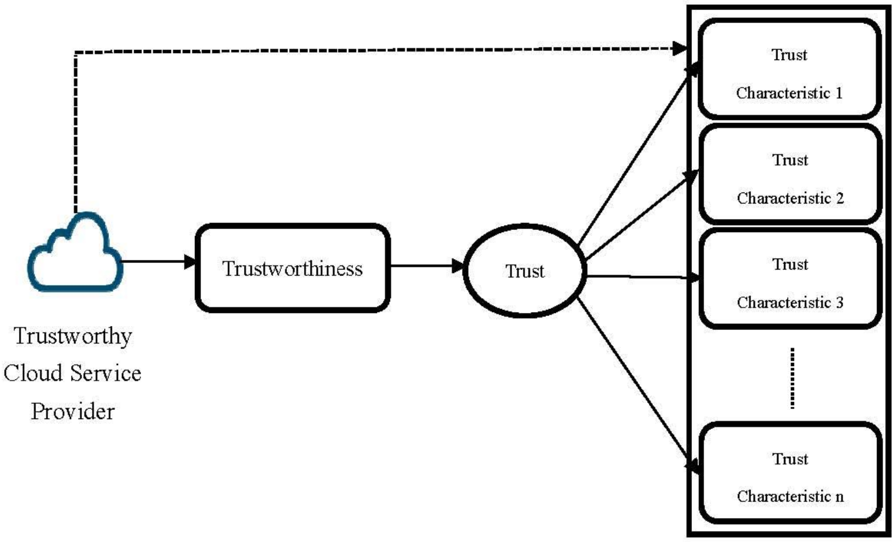


Figure 1. The relationship between trustworthiness, trust, and a trustworthy cloud service provider

3. Related Work

A large and growing body of literature has investigated the role of cloud computing in facilitating data management, sharing hardware and software resources and having a protected interaction between cloud service users and cloud service providers. During the past 20 years much more information has become available on different requirements and challenges in cloud computing. This shows an increasing awareness of the necessity of evaluating the trustworthiness of cloud service providers. Much of the current literature on trust and trustworthiness pay particular attention to evaluate the level of trust in cloud environments. This evaluation is principally done based on some selected characteristics that mainly have direct relationships with users' requirements. However, there is not any criteria or consensus based standard to designate these characteristics precisely (Eftekhar et al., 2018).

Most studies of trust characteristics have only been carried out in one or two aspects of trust (e.g. security (Fernandes, Soares, Gomes, Freire, & Inacio, 2014; Shaikh & Sasikumar, 2015; Subashini & Kavitha, 2011)). Relatively few studies considered security issues along with other characteristics such as availability and reliability (e.g. (Chiregi & Navimipour, 2017)).

Previous studies of trust characteristics have not dealt with the measures of these characteristics comprehensively. For example, Noor et al in (Noor, Sheng, Maamar & Zeadally, 2016) identified trust characteristics of cloud services as authentication, security, privacy, virtualization and accessibility. These characteristics were applied to benchmark four cloud service providers as representative (IBM, Microsoft, Google, and Amazon). In the same vein, Mohammadi et al in (Mohammadi et al., 2013), proposed some trustworthiness characteristics along with their metrics for engineering trusted Internet-based software systems. However, the main weakness of the study is the failure to address how system and software quality standards contribute to these introduced trust characteristics.

On the other hand, Hajizadeh et al in (Hajizadeh & Jafari Navimipour, 2017), measured trust in terms of four characteristics: availability, reliability, interaction evaluation and identity. As discussed in this work, the paper makes no attempt to identify the other aspects of trust. In addition, the author fails to address the measures of each proposed trust characteristics.

Regarding the aforementioned explanations, we have recognized that a work on proposing the measures of the trust characteristics for evaluating cloud services according to the system and software quality standards and cloud computing standards is still the necessity. Following the work which trust characteristics were introduced in (Eftekhar et al., 2018), in this work the measures for each one according to the system and software quality standards are presented.

4. The Main Characteristics Measures to Evaluate Trust in Cloud Computing

In the literature referred to in this paper, the terms ‘measure’ and ‘metric’ are used interchangeably to clarify the important characteristics which can affect trust in cloud environments. Although, they are related, there are some differences. The term ‘measure’ refers to a particular, determined observation of a procedure. Whereas ‘metric’ is defined as the quantifiable elements which are results of measuring. These quantifiable elements are most commonly known as a ratio, percentage or a number. The specific goal of this study is to present the basic set of trust characteristics measures in conformity with cloud computing standards.

Figure 2 illustrates the key trust characteristics of cloud computing proposed in (Eftekhar et al., 2018). These characteristics are divided into ten characteristics and some of them are decomposed into sub-characteristics. To derive these trust characteristics, firstly system and software quality standards and cloud computing standards were investigated. Secondly, by precise analysis of literature, the most frequently proposed trust characteristics by various researchers were identified. Detailed literature and surveyed papers along with the applied methodology can be found in (Eftekhar et al., 2018).

In this paper, we present a holistic way of measuring trust characteristics in cloud environments which allows cloud service users to evaluate subjective (e.g. the user`s previous experience) and objective (e.g. current functionality of the cloud services) trust in cloud computing. In addition, we generalized these trust measures for the three types of cloud service models (Software as a Service, Platform as a Service, Infrastructure as a Service) to create a comprehensive reference for evaluating cloud services proposed by cloud service providers. It should be stressed here that the definitions of the trust characteristics and sub-characteristics are mostly extracted from both cloud computing standard (ISO/IEC 17788 (ISO/IEC, 2014))and system and software quality standards (ISO/IEC 25010 (ISO/IEC, 2011) and ISO/IEC 25011(ISO/IEC, 2017)).

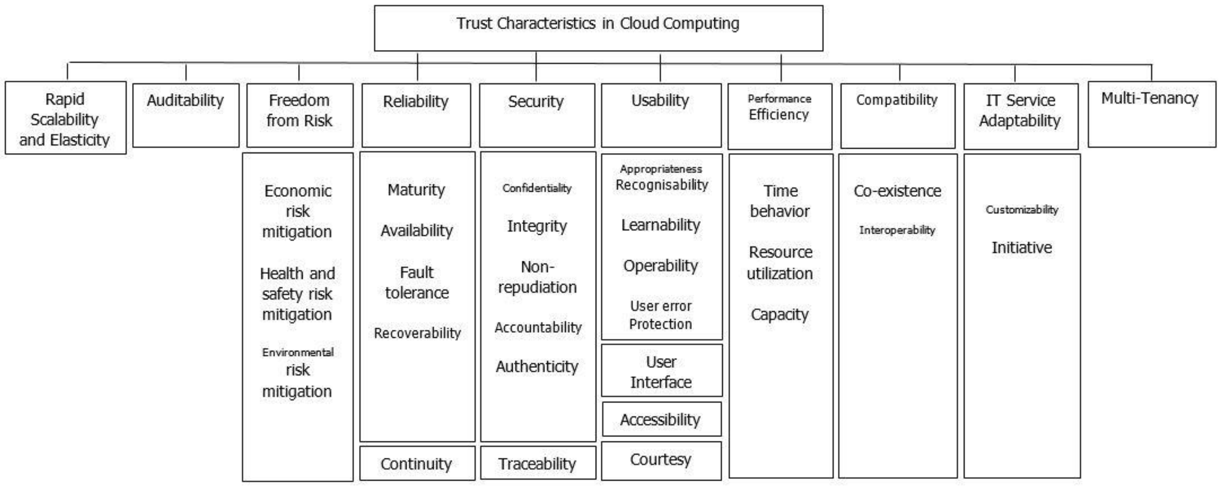


Figure 2. Trust characteristics in cloud computing adapted from (Eftekhar et al., 2018)

4.1 Multi-Tenancy (C4.1)

Resource sharing has a pivotal role in cloud computing. Although, economically it has several significant benefits, it brings several challenges as well. Generally speaking, to provide resource sharing in cloud environments, it may be difficult to distinguish the shareable resources from the isolated ones in cloud environments. Therefore, cloud service providers should be able to offer cloud services that support multi-tenancy. Multi-tenancy is one of the key characteristics of cloud computing and it is defined in ISO/IEC 17788 (ISO/IEC, 2014) as “*a feature where physical or virtual resources are allocated in such a way that multiple tenants and their computations and data are isolated from and inaccessible to one another. Typically, and within the context of multi-tenancy, the group of cloud service users that form a tenant will all belong to the same cloud service customer organization. There might be cases where the group of cloud service users involves users from multiple different cloud service customers, particularly in the case of public cloud and community cloud deployments. However, a given cloud service customer organization might have many different tenancies with a single cloud service provider representing different groups within the organization*”

According to Leymann et al in (Leymann, Schupeck & Arbitter, 2014), to design cloud based applications, the three degrees of multi-tenancy (shared component, tenant-isolated component and dedicated component (Ochei, Bass & Petrovski, 2015)) have to be taken into account. As discussed in this work (Leymann et al., 2014), the main difference is the isolation degree between tenants which is enabled by these patterns. Therefore, isolation has three aspects (Leymann et al., 2014):

1- The performance required by other tenants should not have any effects on the other performance which experienced by a tenant (Performance).

2- The capacity required by one tenant should not have any effects on the capacity available to other tenants (Capacity)

3- The components that belong to a tenant should not be accessible to the other tenants (Confidentiality).

In addition,since the fact of hosting confidential data exposes the system to risks of attacks and security breaches, different researchers have defined multi-tenancy as a security issue in cloud computing (AlJahdali et al., 2014; Khan & Ullah, 2012).

Another important factor that can impact multi-tenancy is scalability and elasticity. Scalability and elasticity refers to quickly increase or decrease resources (ISO/IEC, 2014). In a multi-tenant environment that there are shared resources among tenants, a tenant may require one or more resources from a distant location which are being used by another tenant in different locations. These situations can impact multi tenancy requirements (Bezemer & Zaidman, 2010). Also, the greater scalability and elasticity provided, the better resource sharing requirements can be addressed (Khan & Ullah, 2012).

Therefore, there is a relatively good correlation between multi-tenancy and performance efficiency, security and scalability and elasticity. Accordingly, as scalability and elasticity in ISO/IEC 17788 (ISO/IEC, 2014) are defined as adjusting virtual and physical resources, it can be found that multi-tenancy can be measured by evaluating performance efficiency, security, scalability and elasticity of which their measures are discussed in the following sub-sections.

4.2 Performance Efficiency (C4.2)

Many scholars hold the view that performance efficiency is one of the influential characteristics of cloud services. Accordingly, various researchers evaluate cloud services performance with different measures and perspectives. For example, Villalpando et al in (Villalpando, Abran, Ravanello & Ram ŕez, 2018), introduced a three-dimensional model for measuring performance in cloud computing. The authors in this article proposed the three sub-characteristics of performance efficiency along with the sub-characteristics of reliability in ISO/IEC 25010 as the measures to evaluate performance in cloud environments. However, the paper, makes no attempt to provide information on the measures of these sub-characteristics. On the other hand, the research in the subject which is done by Ataş et al in (Ataş & Gungor, 2014) presented the limited number of performance metrics as following:

- *MFLOPS (Millions of Floating Point Instructions per Second) which is the number of floating-point operations that are performed by CPU in a second.*
- *MOPS (Millions of Operations per Second)*
- *Response Time*
- *Average total operation time for a single record*
- *Average total operation time of 100 records simultaneously*
- *Memory bandwidth*

Regarding the cloud service performance explanation which is provided in cloud computing standard, "*a set of behaviours relating to the operation of a cloud service, and having metrics defined in a SLA*" (ISO/IEC 17788 (ISO/IEC, 2014)), it can be noticed that the metrics which are defined in SLA (Service Level Agreement) have contributed to the measuring the performance of cloud services. Referring to SLA standard (ISO/IEC 19086-1 (ISO/IEC, 2016a)), it can be deduced that the important characteristics to assess performance of the proposed cloud services are (ISO/IEC, 2016a): 1- *cloud service response time (cloud service response time observation, cloud service response time mean, cloud service response time variance),* 2-*capacity (number of simultaneous cloud service connections, limitations of available cloud service resources, cloud service throughput, cloud service bandwidth)* and *3- elasticity (speed, precision).*

To identify measures for evaluating performance in cloud environments, we conducted a 3-stage procedure.

Firstly, considering the definition of performance efficiency as a quality characteristic with three sub-characteristics of time behaviour (SC1), resource utilization (SC2) and capacity (SC3) defined in ISO/IEC 25010 (ISO/IEC, 2011), the important characteristics for cloud service performance mentioned in SLA standard (ISO/IEC 19086-1 [27]), can be mapped to the performance efficiency characteristics in ISO/IEC 25010 (ISO/IEC, 2011). Secondly, the measures for performance characteristic and its sub-characteristics defined in ISO/IEC 25023 (ISO/IEC, 2016c) are extracted. As discussed in this standard (ISO/IEC 25023), the measures for three sub-characteristics of performance efficiency are:

- time behaviour (SC1): mean response time (adapted from ISO/IEC 25023) (m1), response time adequacy (adapted from ISO/IEC 25023) (m2), mean turnaround time (adapted from ISO/IEC 25023) (m3), turnaround time adequacy (adapted from ISO/IEC 25023) (m4), mean throughput (adapted from ISO/IEC 25023) (m5).
- resource utilization (SC2): mean processor utilization (adapted from ISO/IEC 25023) (m6), mean memory utilization (adapted from ISO/IEC 25023) (m7), mean I/O device utilization (adapted from ISO/IEC 25023) (m8), bandwidth utilization (adapted from ISO/IEC 25023) (m9)
- capacity (SC 3): transaction processing capacity (adapted from ISO/IEC 25023) (m10), user access capacity (adapted from ISO/IEC 25023) (m11), user access increase adequacy (adapted from ISO/IEC 25023) (m12)

Thirdly, elasticity (SC4) which was mentioned in SLA standard (ISO/IEC, 2016a) as one of the important characteristics for cloud service performance with its two measures of speed (m13) and provision (m14) (ISO/IEC, 2016a), are considered as the other influential characteristics for performance efficiency.

Speed refers to how fast a cloud service can react to (ISO/IEC, 2016a):1- the cloud user request for re-allocation of resources, -2 changing work load, in the case of manual elasticity and automatic elasticity respectively. Precision is defined in ISO/IEC 19086-1 (ISO/IEC, 2016a) as following:

"*The precision quantity describes how precise the resource allocation meets the actual resource requirements at a given point in time. In the manual case, precision depends on the granularity of the resource allocation, i.e., the minimum amount of resources that can be re-allocated. Hence, in the manual case, precision is a technical characteristic of the cloud service that does not require measurements (i.e., no metric is associated with it). In the automatic case, precision refers to the difference between the amount of resources that are allocated and the amount of resources that are actually needed (the optimum state) to cope with a given workload. The actual resource allocation may be over-provisioned (i.e., more resources are allocated that are actually needed), or under-provisioned (i.e. the amount of resources that are actually allocated is not sufficient to cope with the actual work load). As opposed to the manual case, in the automatic case the difference between the allocated and the actually needed amount of resources can be determined by a measurement process and hence imply a metric.*"

4.3 Security (C4.3)

Despite of the rapid development of cloud computing in many industrial fields in the past decade, cloud environments are still prone to various security risks. Hence, security cannot be ruled out as the first concern in the adoption of cloud computing. Although extensive research has been carried out on evaluating security of the proposed cloud services, more efforts are needed for standardizing the security measures to have a precise evaluation of the proposed cloud services.

Numerous studies have attempted to explain security aspects of cloud environments but there is no endeavor to find the main measures of security characteristics according to the cloud computing standards as well as system and software quality standards. For example, Halabi et al in (Halabi & Bellaiche, 2017) considered confidentiality, integrity, availability and accountability as security aspects or characteristics in a cloud computing environments. Whereas, Abdel-Basset et al in (Abdel-Basset, Mohamed & Chang, 2018) evaluated security according to its correlation to other characteristics.

Security in cloud computing standard (ISO/IEC 17788 (ISO/IEC, 2014)) is one of the key cross-cutting aspects of cloud computing. As explained in (ISO/IEC, 2014), cross-cutting aspects are behaviours that can have effects on activities, components, and multiple roles, and it is not possible to specifically dedicate them to individual roles or components, hence they are apportioned issues among these components and roles. Security in ISO/IEC 17788 (ISO/IEC, 2014) vary from physical security to application security which encompasses needs such as authentication, authorization, availability, confidentiality, identity management, integrity, non-repudiation, audit, security monitoring, incident response, and security policy management. Regarding the sub-characteristics of security depicted in Figure 2(Eftekhar et al., 2018), by mapping security measures extracted from ISO/IEC 25023 (ISO/IEC, 2016c), we summarized the measures of security in cloud computing as following:

- confidentiality (SC1): access controllability (adapted from ISO/IEC 25023) (m1), data encryption correctness (adapted from ISO/IEC 25023) (m2), strength of cryptographic algorithms (adapted from ISO/IEC 25023) (m3)
- integrity (SC2): data integrity (adapted from ISO/IEC 25023) (m4), internal data corruption prevention (adapted from ISO/IEC 25023) (m5), buffer overflow prevention (adapted from ISO/IEC 25023) (m6)
- non-repudiation (SC3): digital signature usage (adapted from ISO/IEC 25023) (m7)
- accountability (SC4): user audit trail completeness (adapted from ISO/IEC 25023) (m8), system log retention (adapted from ISO/IEC 25023) (m9)
- authenticity (SC5): authentication mechanism sufficiency (adapted from ISO/IEC 25023) (m10), authentication rules conformity (adapted from ISO/IEC 25023) (m11)
- traceability (SC6): traceable outcomes (ISO/IEC, 2017) (m12)

4.4 Rapid Scalability and Elasticity (C4.4)

Scalability and elasticity are defined separately in literature with various measures and evaluation methods and have been discussed by a great number of authors in literature. Some significant examples of scalability measures are scalability range, resource scalability rate and cost scalability, and for elasticity measures are usage evolution elasticity, users elasticity speed and mean time to quality repair (Lehrig et al., 2018). Kuhlenkamp et al in (Kuhlenkamp, Klems & Röss, 2014) explained that scalability benchmarking measures performance changes before and after a scaling action and elasticity benchmarking measures performance side-effects of scaling actions. Due to numerous technologies to provide elasticity in cloud computing, Coutinho et al in (Coutinho, Rego, Gomes & de Souza, 2016) proposed some metrics based on *Physics' concepts* to measure elasticity (*strain and stress, and Microeconomics*). Hence, there has been a great deal of confusion in the literature regarding measuring scalability and elasticity in cloud environments. Consequently, referring to cloud computing standard can be a useful guide.

Rapid scalability and elasticity is a key characteristic of cloud computing and in ISO/IEC 17788 (ISO/IEC, 2014) is explained as " *a feature where physical or virtual resources can be rapidly and elastically adjusted, in some cases automatically, to quickly increase or decrease resources. For the cloud service customer, the physical or virtual resources available for provisioning often appear to be unlimited and can be purchased in any quantity at any time automatically, subject to constraints of service agreements. Therefore, the focus of this key characteristic is that cloud computing means that the customers no longer need to worry about limited resources and might not need to worry about capacity planning*." This explanation clarifies three notable concepts. First, scalability and elasticity have a resource-related concept in cloud environments physically or virtually which resource adjustment should be done in a minimum time interval (speed). Second, cloud service customer is legitimate to utilize cloud resources according to the service level agreement (resource utilization) without any disorder or irregularity. Third, regarding the definition of capacity in ISO/IEC 25010 (ISO/IEC, 2011), there should not be any limitation in resource capacity according to the agreement. It means that there should not be any discrepancy between assigned capacity and the required capacity (precision).

Although, scalability is associated with increasing performance when adding further IT resources and does not pay attention to the deletion of these resources, elasticity focuses on the adding and removing of IT resources to adjust systems' performance immediately in case of changing workload (Leymann et al., 2014). Hence, it might be possible to consider scalability as a subset of elasticity in cloud environments. Regarding the aforementioned explanations, it can thus be suggested that performance efficiency with all its measures which was discussed in subsection 4.2 is a reference sub-characteristic of rapid scalability and elasticity.

4.5 Reliability (C4.5)

In the literature, reliability in cloud computing is mostly referred as the ability of a system to provide the required services without failure or interruption (Sharma, Javadi, Si & Sun, 2016). It is also known as the probability of all the applications or data resources to involve in the executing the required services successfully (Cui, Li, Liu, Ansari & Liu, 2017). Regarding these definitions, it can be deduced that fault tolerance is the only measure for reliability in cloud computing. Such expressions are unsatisfactory because they fail to acknowledge the significance of the other measures as mentioned in ISO/IEC 25010 (ISO/IEC, 2011) (Figure 2).

A more accurate definition of reliability can be found in ISO/IEC 25010 (ISO/IEC, 2011) that is "*degree to which a system, product or component performs specified functions under specified conditions for a specified period of time*."Therefore, to evaluate the cloud service reliability, the measures adapted from ISO/IEC 25010

(ISO/IEC, 2011) and ISO/IEC 25023 for it's sub-characteristics which are illustrated in Figure 2 (Eftekhar et al., 2018), are proposed as following (ISO/IEC, 2016c, 2017):

- maturity (SC1): fault correction (adapted from ISO/IEC 25023) (m1), mean time between failure (adapted from ISO/IEC 25023) (m2), failure rate (adapted from ISO/IEC 25023) (m3), test coverage (adapted from ISO/IEC 25023) (m4)
- availability (SC2): system availability (adapted from ISO/IEC 25023) (m5), mean down time (adapted from ISO/IEC 25023) (m6)
- fault tolerance (SC3): failure avoidance (adapted from ISO/IEC 25023) (m7), redundancy of components (adapted from ISO/IEC 25023) (m8), mean fault notification time (adapted from ISO/IEC 25023) (m9)
- recoverability (SC4): mean recovery time (adapted from ISO/IEC 25023) (m10), backup data completeness (adapted from ISO/IEC 25023) (m11)
- continuity (ISO/IEC, 2017) (SC5): supported cloud services (m12) (The percentage of the supported cloud services. e.g. to mitigate the risks resulting from interruption to an acceptable level)

4.6 Freedom from Risk (C4.6)

As mentioned in the literature, selection of a trustworthy cloud service provider is a decision-making problem. Therefore, making a decision meticulously needs risk analysis, control and mitigation (Heckmann, Comes & Nickel, 2015). But, to the best of our knowledge, 'freedom from risk' as a trust characteristic to evaluate in cloud environments is significantly overlooked in the literature.

From monetary perspective, cloud computing causes cost saving and reduces expenditures. This notable benefit of cloud technology is a pivotal reason for the organizations to switch to cloud environments (Ali, Warren & Mathiassen, 2017). But as return on investment (ROI) is a long term goal (Venters & Whitley, 2012), and during this period, many individuals and stakeholders may be attracted and migrate their data to cloud environments, neglecting this characteristic (freedom from risk) can lead to irreparable damages such as very huge financial losses, disclosing information and confidential data, wasting time and human resources.

In broad terms, risk is the probability of a perilous case occurrence that can have an effect on the achieving goals (Djemame, Armstrong, Guitart & Macias, 2016). *Consequence* or *impact* and *likelihoodof the event* are the main factors for risk measuring (Misra, 2008). As explained in ISO/IEC 25022 (ISO/IEC, 2016b), inadequacy of any product quality characteristic or inadequate levels of effectiveness and efficiency can cause the risks of undesirable consequences. In addition, risks of undesirable consequences can have impacts on the user of a system, organizations which are using a system, organizations that are developing a system and a wider community (ISO/IEC, 2016b).

Accordingly, freedom from risk in ISO/IEC 25010 (ISO/IEC, 2011), is "*degree to which a product or system mitigates the potential risk to economic status, human life, health, or the environment*". Regarding its sub-characteristics depicted in figure 2, measures for evaluating this characteristic (freedom from risk) are explained as following (ISO/IEC, 2016b):

- economic risk mitigation (SC1): return on investment (adapted from ISO/IEC 25022) (ROI) (m1), time to achieve return on investment (adapted from ISO/IEC 25022) (m2), business performance (adapted from ISO/IEC 25022) (m3), benefits of IT investment (adapted from ISO/IEC 25022) (m4), service to customers (adapted from ISO/IEC 25022) (m5), cloud customers loyal to a specific cloud service provider (m6) (the percentage of the loyal cloud customers compared to all the customers of a specific cloud service provider), revenue from each customer (adapted from ISO/IEC 25022) (m7), errors with economic consequences (adapted from ISO/IEC 25022) (m8)
- health and safety risk mitigation (SC2): user health reporting frequency (adapted from ISO/IEC 25022) (m9), user health and safety impact (adapted from ISO/IEC 25022) (m10), safety of people affected by use of the system (adapted from ISO/IEC 25022) (m11)
- environmental risk mitigation (SC3): environmental impact (adapted from ISO/IEC 25022) (m12)

4.7 Usability (C4.7)

Regarding the competitive atmosphere among cloud service providers for attracting customers, usability is a key aspect for addressing users' requirements. Thus, evaluating usability is the hidden characteristic to thrive in this competitive environment (Roy, Pattnaik & Mall, 2017). Moreover, since there are different cloud deployment models without stability to the users' experience, it is being remarkably recognized by cloud service users that enhancing cloud usability standards is necessary to certify stability among various cloud services proposed by diverse cloud service providers (Stanton, Theofanos & Joshi, 2015).

Usability is an attribute of a product that measures to what extent it can be usable by different users with *efficiency*, *effectiveness* and *satisfaction* to achieve their determined goals (ISO 1998a) (Pandey & Daniel, 2016). Also usability refers to the ability of a product to be understood, learned, operated and is habitually verified from its interfaces (Baharuddin, Singh & Razali, 2013; Thomas, Onyimbo & Logeswaran, 2016). More specifically, usability in ISO/IEC 25010 (ISO/IEC, 2011), is defined as "*degree to which a product or system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use*". To evaluate usability, the measures for its sub-characteristics (Figure 2) which are extracted from ISO/IEC 25023 (ISO/IEC, 2016c) explained as following, should be taken into account.

- appropriateness recognisability (SC1): description completeness (adapted from ISO/IEC 25023) (m1), demonstration coverage (adapted from ISO/IEC 25023) (m2), entry point self-descriptiveness (adapted from ISO/IEC 25023) (m3)
- learnability(SC2): user guidance completeness (adapted from ISO/IEC 25023) (m4), entry fields defaults (adapted from ISO/IEC 25023) (m5), error message understandability (adapted from ISO/IEC 25023) (m6), self-explanatory user interface (adapted from ISO/IEC 25023) (m7)
- operability(SC3): operational consistency (adapted from ISO/IEC 25023) (m8), message clarity (adapted from ISO/IEC 25023) (m9), functional customizability (adapted from ISO/IEC 25023) (m10), user interface customizability (adapted from ISO/IEC 25023) (m11), monitoring capability (adapted from ISO/IEC 25023) (m12), undo capability (adapted from ISO/IEC 25023) (m13), understandable categorization of information (adapted from ISO/IEC 25023) (m14), appearance consistency (adapted from ISO/IEC 25023) (m15), input device support (adapted from ISO/IEC 25023) (m16)
- user error protection(SC4): avoidance of user operation errors (adapted from ISO/IEC 25023) (m17), user entry error correction (adapted from ISO/IEC 25023) (m18), user error recoverability (adapted from ISO/IEC 25023) (m19)
- user interface aesthetics (SC5): appearance aesthetics of user interfaces (adapted from ISO/IEC 25023) (m20)
- accessibility(SC6): accessibility for users with disabilities (adapted from ISO/IEC 25023) (m21), supported languages adequacy (adapted from ISO/IEC 25023) (m22)
- courtesy (ISO/IEC, 2017) (SC7): customer supports experience (m23)

4.8 Compatibility (C4.8)

Cloud computing enables ubiquitous network access to the shared resources (Mell & Grance, 2011), hence, there is a possibility that by producing new opportunities, makes some challenges as well. One of these challenges is compatibility with customers' components and services; i.e. the proposed cloud services must align with customers' requirements, outcomes, frameworks, policy and environment (Ali et al., 2017; Lin & Chen, 2012). In addition, it is believed that by the alignment of the cloud computing platforms with the Internet platform more precisely, the capacity to take the advantages of cloud computing will be developed and also the level of skepticism among the individuals and organizations for using cloud services, will be reduced significantly (Gangwar, Date & Ramaswamy, 2015). From users' perspective, in case of using a single cloud service which is not able to completely address users' needs, inevitably, combining cloud services from different cloud providers is an alternative (Dastjerdi & Buyya, 2014). But checking the compatibility of the other cloud services proposed by various providers can be a challenging task particularly, for non-expert users (Dastjerdi & Buyya, 2014). Therefore, to evaluate the compatibility of a cloud service, as defined in ISO/IEC 25010 (ISO/IEC, 2011) as "*degree to which a product, system or component can exchange information with other products, systems or components, and/or perform its required functions, while sharing the same hardware or software environment*" and regarding its sub-characteristics depicted in Figure 2, its measures extracted from ISO/IES 25023 (ISO/IEC, 2016c) can be presented as following:

- co-existence (SC1): co-existence with other cloud services (adapted from ISO/IEC 25023) (m1) (in what extend the determined cloud service can share the environment with other cloud services without adverse impact on their quality characteristics or functionality).
- interoperability(SC2): data format exchangeability (adapted from ISO/IEC 25023) (m2) (the proportion of the specified data formats is exchangeable with other cloud services), data exchange protocol sufficiency (adapted from ISO/IEC 25023) (m3), external interface adequacy (adapted from ISO/IEC 25023) (m4)

4.9 IT Service Adaptability (C4.9)

In ISO/IEC 25011 (ISO/IEC, 2017), IT service adaptability is defined as "*degree to which an IT service can configure itself or be modified to meet new needs*". In terms of time, having new needs refers to the fact that there are two types of requirements: 1- actual requirements: the determined requirements of the users before using cloud services, 2- future requirements: the requirements that users will come across deliberately or accidentally after the adoption of a cloud service proposed by a cloud service provider. Therefore, as discussed in ISO/IEC 25011 (ISO/IEC, 2017) and depicted in Figure 2 (Eftekhar et al., 2018), customizability and initiative are the main sub-characteristics of IT service adaptability. To cover future requirements, the proposed cloud service must be adaptable and to ensure the IT service adaptability, it should be measured. Regarding the three well-known service models in cloud computing (i.e. Software as a Service, Platform as a Service, and Infrastructure as a Service), hardware and software adaptability of the proposed cloud services should be considered. This is one of the momentous aspects of trust in cloud environments that can satisfy different types of user's requirements. The important measures of this characteristic are as following (ISO/IEC, 2016c):

- customizability(SC1): functional customizability (m1), hardware customizability (m2), software customizability (m3), operational environment customizability (m4)
- initiative(SC2): changeability of the cloud service (m5)

4.10 Auditability (C4.10)

Auditing is generally seen as a characteristic strongly related to assure users that the proposed cloud services have the acceptable quality (or not). In addition, the results of auditing can be an important determinant in the cloud service provider selection. In the literature, there are numerous ways for auditing cloud services and cloud service providers. However, a closer look at the literature on the contributory characteristics to conduct a rigorous auditing, reveals a number of gaps and shortcomings.

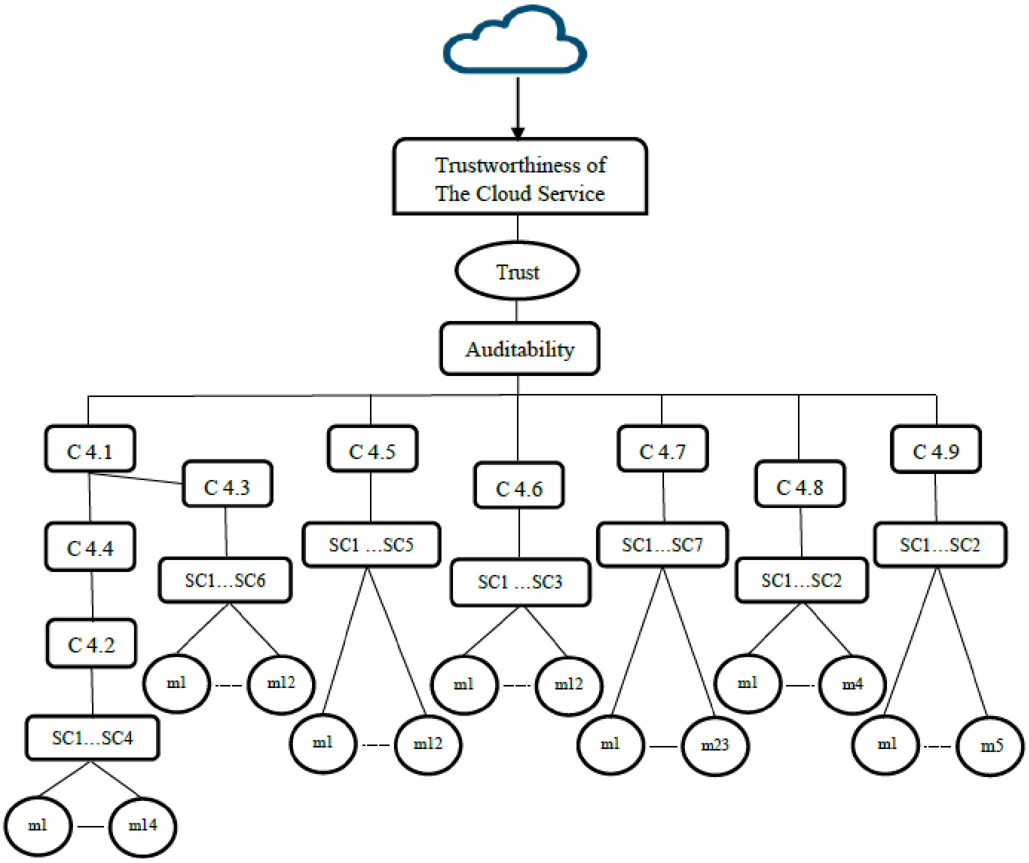
Referring to ISO/IEC 17788 (ISO/IEC, 2014), auditability is "*the capability of collecting and making available necessary evidential information related to the operation and use of a cloud service, for the purpose of conducting an audit*". Therefore, based on the aforementioned explanations, it can be simply justified that evaluating the auditability of the proposed cloud services stems from evaluating the necessary characteristics of cloud services which are explained in previous subsections.

5. Results and Discussion

Basically, the trust characteristics presented in the literature, are related to the principal aspects of cloud computing. However, the measures we found in the literature for assessing the proposed trust characteristics do not conform to system and software quality standards, nor are they easily applied to the context of cloud computing. Since there is no rule to select cloud trust characteristics measures, we chose instead to refer to existing standards and identify these measures. We chose these standards as they are agreed-upon reference, available, and have scientific and academic support.

On the other hand, to date, the existing literature on trust characteristics and their measures are mostly based on the authors' perspectives by their analysis of the literature. But this approach may not be comprehensive enough in order to evaluate trust in cloud environments, since there may be some inconsistencies and discrepancies while proposing trust characteristics and their measures (e.g. (Fiandrino, Kliazovich, Bouvry & Zomaya, 2017), (Qiu, Dai, Xiang & Xing, 2016)).

The present study aimed to determine the measures of trust characteristics based on analyzing standard characteristics of cloud computing and IT services, extracted from system and software quality standards and cloud computing standards. Figure 3, illustrates the trust tree of cloud computing along with the standard measures which are proposed in this article. This trust tree is complementary to work (Eftekhar et al., 2018) results of which are depicted in Figure 2.



C 4.1/…/ C 4.9	Characteristics: Each characteristic is depicted by its number of sub-section in this article.
SC	Sub-Characteristics of each trust characteristic.
m 1/…/m 23	Leafs: Measures of each sub-characteristic.

C 4.1: Multi-Tenancy
C 4.2: Performance Efficiency
C 4.3: Security
C 4.4: Rapid Scalability and Elasticity
C 4.5: Reliability
C 4.6: Freedom from Risk
C 4.7: Usability
C 4.8: Compatibility
C 4.9: IT Service Adaptability

Figure 3. The trust tree of cloud computing

As depicted in Figure 3, auditability is placed as the sub-layer of trust which is the measure of trustworthiness in cloud computing. We decided to place it here since the evaluation of cloud services by cloud providers may be complicated by dishonesty on the part of the service providers (Huang & Nicol, 2013). This can be the main problem in the cloud computing adoption. Therefore, outsourcing the auditing cloud services to a trusted third party can produce more trustworthy results. Taking into account this fact, it can thus be concluded that by outsourcing auditing procedures, users are searching for a way to boost their confidence about cloud service provider selection and to ensure that the selected cloud services can cover the determined requirements. In the light of these principles and regarding the definition of trust in the system/software quality standard (ISO/IEC 25010 (ISO/IEC, 2011)), namely, "*the degree to which a user or other stakeholder has confidence that a product or system will behave as intended*", the correlation between trust and auditability can clearly be justified. Moreover, auditability of the system can be assumed as a gateway in it's evaluation. If this gateway does not exist in the system, there is a possibility that the system may be unavailable for any form of real, fact-based evaluation.

The presented trust tree can be considered as complete as possible trust characteristics reference in the time of conducting this research, along with the associated measures in cloud environments. What remains is for the proposed trust characteristics measures to be applied to real scenarios in order to assess their applicability in evaluating the trustworthiness of the cloud service provider. The presented measures can be used to evaluate both subjective (e.g. the user`s previous experience) and objective (e.g. current functionality of the cloud services) trust in cloud environments.

6. Conclusion

The literature has highlighted several methods to define measures for evaluating trust characteristics in cloud computing. However, all the previously mentioned methods suffer from some serious shortcomings that we aimed to address. First, we cannot neglect the contribution of the existing related ISO/IEC standards when establishing measures for cloud trust characteristics. Second, there are various methods proposed by different researchers that are completely inapplicable to evaluate trust characteristics in cloud environments, since they lack scientifically supported measures. Third, because the notion of trust also has uncertainty associated with it, combining both subjective and objective evaluation of trust in cloud environments we can achieve a more credible outcome.

We analyzed cloud computing standards as well as system/software quality standards in order to extract measures for evaluating the proposed trust characteristics in cloud computing. We reviewed the literature on evaluating these characteristics in cloud environments to conform the proposed measures to various perspectives. The result of this conformity is depicted as a trust tree to be considered as a reference for evaluating trust in cloud environments.

It should be noted that the result of this study would be a fruitful area for further work. More broadly, research is also needed to determine the applicability of the proposed characteristics with their measures in cloud computing. More information on trust characteristics measures would be helpful to establish a greater degree of accuracy on this matter.

Moving forward, a natural progression of this work is to propose a cloud trust model to evaluate the proposed trust characteristics according to their identified measures.

Acknowledgment

We would like to express our gratitude to Mehran Panahi Osalo for his constructive feedback.

References

Abdel-Basset, M., Mohamed, M., & Chang, V. (2018). NMCDA: A framework for evaluating cloud computing services. *Future Generation Computer Systems, 86*, 12-29. https://doi.org/10.1016/j.future.2018.03.014

Ali, A., Warren, D., & Mathiassen, L. (2017). Cloud-based business services innovation: A risk management model. *International Journal of Information Management, 37*(6), 639-649. https://doi.org/10.1016/j.ijinfomgt.2017.05.008

AlJahdali, H., Albatli, A., Garraghan, P., Townend, P., Lau, L., & Xu, J. (2014). *Multi-tenancy in cloud computing.* Paper presented at the Service Oriented System Engineering (SOSE), 2014 IEEE 8th International Symposium on. https://doi.org/10.1109/SOSE.2014.50

Ataş, G., & Gungor, V. C. (2014). Performance evaluation of cloud computing platforms using statistical methods. *Computers & Electrical Engineering, 40*(5), 1636-1649. https://doi.org/10.1016/j.compeleceng.2014.03.017

Baharuddin, R., Singh, D., & Razali, R. (2013). Usability dimensions for mobile applications—a review. *Res. J. Appl. Sci. Eng. Technol, 5*(6), 2225-2231. https://doi.org/10.19026/rjaset.5.4776

Bezemer, C.-P., & Zaidman, A. (2010). *Multi-tenant SaaS applications: maintenance dream or nightmare?* Paper presented at the Proceedings of the Joint ERCIM Workshop on Software Evolution (EVOL) and International Workshop on Principles of Software Evolution (IWPSE). https://doi.org/10.1145/1862372.1862393

Chahal, R. K., & Singh, S. (2017). Fuzzy rule-based expert system for determining trustworthiness of cloud service providers. *International Journal of Fuzzy Systems, 19*(2), 338-354. https://doi.org/10.1007/s40815-016-0149-1

Chiregi, M., & Navimipour, N. J. (2017). A comprehensive study of the trust evaluation mechanisms in the cloud computing. *Journal of Service Science Research, 9*(1), 1-30. https://doi.org/10.1007/s12927-017-0001-7

Coutinho, E. F., Rego, P. A., Gomes, D. G., & de Souza, J. N. (2016). Physics and microeconomics-based metrics for evaluating cloud computing elasticity. *Journal of network and computer applications, 63*, 159-172. https://doi.org/10.1016/j.jnca.2016.01.015

Cui, H., Li, Y., Liu, X., Ansari, N., & Liu, Y. (2017). Cloud service reliability modelling and optimal task scheduling. *IET Communications, 11*(2), 161-167. https://doi.org/10.1049/iet-com.2016.0417

Dastjerdi, A. V., & Buyya, R. (2014). Compatibility-aware cloud service composition under fuzzy preferences of users. *IEEE transactions on cloud computing, 2*(1), 1-13. https://doi.org/10.1109/TCC.2014.2300855

Djemame, K., Armstrong, D., Guitart, J., & Macias, M. (2016). A risk assessment framework for cloud computing. *IEEE transactions on cloud computing*(1), 1-1. https://doi.org/10.1109/TCC.2014.2344653

Eftekhar, S. M., Suryn, W., Roy, J., & Terfas, H. (2018). Towards the Development of a Widely Accepted Cloud Trust Model. *SQM XXVI*, 73.

Fan, W.-J., Yang, S.-L., Perros, H., & Pei, J. (2015). A multi-dimensional trust-aware cloud service selection mechanism based on evidential reasoning approach. *International Journal of Automation and Computing, 12*(2), 208-219. https://doi.org/10.1007/s11633-014-0840-3

Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inacio, P. R. M. (2014). Security issues in cloud environments: a survey. *International Journal of Information Security, 13*(2), 113-170. https://doi.org/10.1007/s10207-013-0208-7

Fiandrino, C., Kliazovich, D., Bouvry, P., & Zomaya, A. Y. (2017). Performance and energy efficiency metrics for communication systems of cloud computing data centers. *IEEE transactions on cloud computing, 5*(4), 738-750. https://doi.org/10.1109/TCC.2015.2424892

Gangwar, H., Date, H., & Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. *Journal of Enterprise Information Management, 28*(1), 107-130. https://doi.org/10.1108/JEIM-08-2013-0065

Gonzales, D., Kaplan, J. M., Saltzman, E., Winkelman, Z., & Woods, D. (2017). Cloud-trust—A security assessment model for infrastructure as a service (IaaS) clouds. *IEEE transactions on cloud computing, 5*(3), 523-536. https://doi.org/10.1109/TCC.2015.2415794

Habib, S. M., Hauke, S., Ries, S., & Mühlhäuser, M. (2012). Trust as a facilitator in cloud computing: a survey. *Journal of Cloud Computing: Advances, Systems and Applications, 1*(1), 19. https://doi.org/10.1186/2192-113X-1-19

Hajizadeh, R., & Jafari Navimipour, N. (2017). A method for trust evaluation in the cloud environments using a behavior graph and services grouping. *Kybernetes*(just-accepted), 00-00. https://doi.org/10.1108/K-02-2017-0070

Halabi, T., & Bellaiche, M. (2017). Towards quantification and evaluation of security of Cloud Service Providers. *Journal of Information Security and Applications, 33*, 55-65. https://doi.org/10.1016/j.jisa.2017.01.007

Heckmann, I., Comes, T., & Nickel, S. (2015). A critical review on supply chain risk–Definition, measure and modeling. *Omega, 52*, 119-132. https://doi.org/10.1016/j.omega.2014.10.004

Huang, J., & Nicol, D. M. (2013). Trust mechanisms for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications, 2*(1), 9. https://doi.org/10.1186/2192-113X-2-9

ISO/IEC. (2011). 25010 (2011) Systems and software engineering-Systems and software Quality Requirements and Evaluation (SQuaRE)-System and software quality models. *International Organization for Standardization, Geneva, Switzerland*.

ISO/IEC. (2014). 17788 (2014) Information technology — Cloud computing — Overview and vocabulary. *International Organization for Standardization, Geneva, Switzerland*.

ISO/IEC. (2016a). 19086-1,Information technology — Cloud computing — Service level agreement (SLA) framework and technology — Part 1: Overview and concepts. *International Organization for Standardization, Geneva, Switzerland*.

ISO/IEC. (2016b). 25022 (2016) Systems and software engineering — Systems and software quality requirements and evaluation (SQuaRE) — Measurement of quality in use. *International Organization for Standardization, Geneva, Switzerland*.

ISO/IEC. (2016c). 25023 (2016) Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Measurement of system and software product quality. *International Organization for Standardization, Geneva, Switzerland*.

ISO/IEC. (2017). 25011 (2017) - Information technology — Systems and software quality requirements and evaluation (SQuaRE) — Service quality models. *International Organization for Standardization, Geneva, Switzerland*.

Khan, M. F., & Ullah, M. A. (2012). An approach towards customized multi-tenancy. *International Journal of Modern Education and Computer Science (IJMECS)[online], 4*(9), 39. https://doi.org/10.5815/ijmecs.2012.09.05

Kuhlenkamp, J., Klems, M., & Röss, O. (2014). Benchmarking scalability and elasticity of distributed database systems. *Proceedings of the VLDB Endowment, 7*(12), 1219-1230. https://doi.org/10.14778/2732977.2732995

Lehrig, S., Sanders, R., Brataas, G., Cecowski, M., Ivanšek, S., & Polutnik, J. (2018). CloudStore—towards scalability, elasticity, and efficiency benchmarking and analysis in Cloud computing. *Future Generation Computer Systems, 78*, 115-126. https://doi.org/10.1016/j.future.2017.04.018

Leymann, C. F. F., Schupeck, R. R. W., & Arbitter, P. (2014). (Book) Cloud Computing Patterns. *Springer*.

Li, Z., Liao, L., Leung, H., Li, B., & Li, C. (2017). Evaluating the credibility of cloud services. *Computers & Electrical Engineering, 58*, 161-175. https://doi.org/10.1016/j.compeleceng.2016.05.014

Lin, A., & Chen, N.-C. (2012). Cloud computing as an innovation: Percepetion, attitude, and adoption. *International Journal of Information Management*, *32*(6), 533-540. https://doi.org/10.1016/j.ijinfomgt.2012.04.001

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

Misra, K. B. (2008). *Handbook of performability engineering*: Springer Science & Business Media. https://doi.org/10.1007/978-1-84800-131-2

Mohammadi, N. G., Paulus, S., Bishr, M., Metzger, A., Könnecke, H., Hartenstein, S., . . . Pohl, K. (2013). *Trustworthiness attributes and metrics for engineering trusted internet-based software systems.* Paper presented at the International Conference on Cloud Computing and Services Science.

Noor, T. H., Sheng, Q. Z., Maamar, Z., & Zeadally, S. (2016). Managing trust in the cloud: state of the art and research challenges. *Computer*(2), 34-45. https://doi.org/10.1109/MC.2016.57

Ochei, L. C., Bass, J. M., & Petrovski, A. (2015). *Evaluating degrees of multitenancy isolation: A case study of cloud-hosted gsd tools.* Paper presented at the Cloud and Autonomic Computing (ICCAC), 2015 International Conference on. https://doi.org/10.1109/ICCAC.2015.17

Pandey, S., & Daniel, A. (2016). *Fuzzy logic based cloud service trustworthiness model.* Paper presented at the Engineering and Technology (ICETECH), 2016 IEEE International Conference on. https://doi.org/10.1109/ICETECH.2016.7569215

Qiu, X., Dai, Y., Xiang, Y., & Xing, L. (2016). A hierarchical correlation model for evaluating reliability, performance, and power consumption of a cloud service. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 46*(3), 401-412. https://doi.org/10.1109/TSMC.2015.2452898

Rajendran, V. V., & Swamynathan, S. (2016). Hybrid model for dynamic evaluation of trust in cloud services. *Wireless Networks, 22*(6), 1807-1818. https://doi.org/10.1007/s11276-015-1069-y

Roy, S., Pattnaik, P. K., & Mall, R. (2017). Quality assurance of academic websites using usability testing: an experimental study with AHP. *International Journal of System Assurance Engineering and Management, 8*(1), 1-11. https://doi.org/10.1007/s13198-016-0436-0

Shaikh, R., & Sasikumar, M. (2015). Trust model for measuring security strength of cloud computing service. *Procedia Computer Science, 45*, 380-389. https://doi.org/10.1016/j.procs.2015.03.165

Sharma, Y., Javadi, B., Si, W., & Sun, D. (2016). Reliability and energy efficiency in cloud computing systems: Survey and taxonomy. *Journal of network and computer applications, 74*, 66-85. https://doi.org/10.1016/j.jnca.2016.08.010

Singh, S., & Sidhu, J. (2017). Compliance-based multi-dimensional trust evaluation system for determining trustworthiness of cloud service providers. *Future Generation Computer Systems, 67*, 109-132. https://doi.org/10.1016/j.future.2016.07.013

Stanton, B., Theofanos, M., & Joshi, K. P. (2015). *Framework for cloud usability.* Paper presented at the International Conference on Human Aspects of Information Security, Privacy, and Trust. https://doi.org/10.1007/978-3-319-20376-8_59

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, *34*(1), 1-11. https://doi.org/10.1016/j.jnca.2010.07.006

Suryn, W. (2013). Software quality engineering: a practitioner's approach: John Wiley & Sons.

Sztompka, P. (1999). Trust: A sociological theory: Cambridge University Press.

Thomas, M. O., Onyimbo, B. A., & Logeswaran, R. (2016). Usability evaluation criteria for internet of things. *International Journal of Information Technology and Computer Science, 8*(12), 10-18. https://doi.org/10.5815/ijitcs.2016.12.02

Venters, W., & Whitley, E. A. (2012). A critical review of cloud computing: researching desires and realities. *Journal of Information Technology, 27*(3), 179-197. https://doi.org/10.1057/jit.2012.17

Villalpando, L. E. B., Abran, A., Ravanello, A., & Ram ŕez, A. E. (2018). A Three-Dimensional Performance Measurement Model for Cloud Computing. *Journal of Software Engineering and Applications, 11*(05), 235. https://doi.org/10.4236/jsea.2018.115015